

QUANTA: QUantum Analytical Network Testing & Assessment

Jinchen Ma, Clive Marvelous, James McDougall,
Jake Smith, Zhu Xu, Haoran Zhang



Executive Summary: The Report reviews state-of-the-art simulation methods for time-bin entangled quantum networks and introduces QUANTA, an educational simulation tool that illustrates the fundamental hardware and networking concepts of entanglement distribution. QUANTA supports the simulation of single entanglement links, repeater chains, and larger entangled networks. Recent works modelling quantum network devices, such as entangled sources, quantum memory, and quantum error correction (QEC), are integrated into a repeater chain architecture to evaluate performance with realistic devices compared to idealised hardware models. QUANTA's capabilities are demonstrated by: comparing the relative performance of recent experimental demonstrations of quantum memories within repeater chains; exploring methods to optimise repeater chain performance, including fibre multiplexing and improved entanglement-swapping schemes, for applications such as Quantum Key Distribution (QKD); presenting a potential resource allocation scheme within larger entangled networks to enable simultaneous network utilization by all users; and evaluating the trade-offs of incorporating QEC to improve entanglement fidelity at the cost of distribution rate. By integrating realistic hardware devices into repeater chains, QUANTA can estimate network performance as devices progress and evaluate the trade-off between improving the performance of current-generation devices with link optimisation methods and the greater link complexity and management overhead they impose.

Supervised by Dr. S. Joshi.

School of Electrical, Electronic and Mechanical Engineering
UNIVERSITY OF BRISTOL

2025

Declaration

This project report is submitted towards an application for a degree at the University of Bristol. The report is based upon independent work by the candidates. All contributions from others have been acknowledged and the supervisor is identified on the front page. The views expressed within the report are those of the authors and not of the University of Bristol. We hereby assert our right to be identified as the authors of this report. We give permission to the University of Bristol Library to add this report to its stock and to make it available for consultation in the library, and for inter-library lending for use in another library. It may be copied in full or in part for any bona fide library or research worker on the understanding that users are made aware of their obligations under copyright legislation. We hereby declare that the above statements are true.

Jinchen Ma: _____

Clive Marvelous: _____

James McDougall: _____

Jake Smith: _____

Zhu Xu: _____

Haoran Zhang: _____

© Copyright Jinchen Ma, Clive Marvelous, James McDougall, Jake Smith, Zhu Xu, Haoran Zhang 2025.

Certification of ownership of the copyright in a dissertation presented as part of and in accordance with the requirements for the relevant degree at the University of Bristol.

This report is the property of the University of Bristol Library and may only be used with due regard to the authors.

Bibliographical references may be noted but no part may be copied for use or quotation in any published work without prior permission of the authors. In addition, due acknowledgement for any use must be made.

Work Allocation

- Jinchen Ma (JMa): Responsible for addressing error processes in long-distance QKD by employing quantum error correction (QEC) to proactively protect information against noise in both quantum channels and quantum memories, preventing physical errors from propagating. In parallel, implemented entanglement purification (EP) to upgrade imperfect entangled states to higher fidelity. Designed distinct QEC schemes for channel- and memory-induced noise, and developed a modular EP suite with multiple protocols. A multi-dimensional evaluation framework is provided so users can compare alternatives along different considerations and select the option that best fits their requirements.
- Clive Marvelous (CM): Responsible for the theoretical modelling and integration of quantum memories within the simulator. This involved implementing different protocols and platforms, defining their parameters and ensuring consistent interaction with other components. Additional tasks included setting modelling assumptions and providing users with flexible parameters to explore performance trade-offs.
- James McDougall (JMc): Took the lead on GUI development and managing the simulation code produced by other group members with git. Linked front-end GUI code to back-end simulation and validated simulation results when run through the GUI. Reviewed literature surrounding basic single link entanglement networks. Assisted Jake in the development of the back-end single link simulation model and analysed and validated results for single link characterisation.
- Jake Smith (JS): Conducted a literature review to determine suitable modelling methodologies and device parameters for quantum communication devices, links, and repeater chain. Derived additional modelling methods, such as adapting Guha's [1] repeater architectures to support realistic source and detector parameters. Performed analytical investigations to characterize links and repeaters based on competing source and detector configurations, and the allocation of entangled resources in a network. Integrated other members work into the simulator to perform joint analytical investigations to characterize repeaters with noisy quantum memory and entanglement purification.
- Zhu Xu (ZX): Responsible for theoretical modeling and structural framework design of entanglement swapping relay chains and trusted node relay chains. Extended Guha's structural models and mathematical formulations to conduct comprehensive analytical analysis of three mainstream protocols in entanglement swapping. Investigated the feasibility of WDM technology and collaborated with team members on simulation of related results. Additionally, developed a simulation class library for trusted relay chains and performed numerical simulation analysis of key generation rate characteristics.
- Haoran Zhang (HZ): Quantum communication networks based on the E91 entanglement protocol are modeled and analyzed over a broad range of end-to-end distances. Secret-key rate and quantum bit error rate (QBER) are evaluated for single links, repeater chains, and mesh topologies. A unified framework consolidates models and computation, specifies key device/channel parameters, and reproduces published single-link results. Recursive expressions extend QBER and key-rate analysis to repeater chains; the method is applied to ring and two-dimensional lattice networks to evaluate arbitrary node pairs.

We confirm that the information on this page accurately describes our individual contributions to the project.

Jinchen Ma: _____ Clive Marvelous: _____

James McDougall: _____ Jake Smith: _____

Zhu Xu: _____ Haoran Zhang: _____

Contents

	Page
1 Introduction	5
1.1 Motivation (JMc)	5
1.2 Objectives (JMc)	5
2 Background	6
2.1 Quantum Link Devices (JS)	6
2.2 Quantum Repeater Network Structures (ZX, HZ)	7
2.3 Quantum Optical Memory (CM)	9
2.4 Quantum Frequency Converter (CM)	11
2.5 Quantum Error Mitigation Strategies (JMa)	12
2.6 GUI Development (JMc)	12
3 Methods	15
3.1 Software Structure and Implementation (JMc)	15
3.2 Single Link Modelling (JS, CM)	18
3.3 Quantum Repeater Chain (ZX, JS)	20
3.4 Trusted Node Chain (ZX)	26
3.5 QM Mathematical Model for EIT and Off-Resonant Raman (CM)	27
3.6 Quantum Error Correction (JMa)	28
3.7 Entanglement Purification Module (JMa)	30
3.8 Integration of Models in the Simulator (JS, JMc, JMa)	35
3.9 Limitations of QUANTA	35
3.10 Comparing QUANTA with Other Quantum Network Simulators (JS):	36
4 Results	37
4.1 Single Link Hardware Characterization (JS, JMc)	37
4.2 Characterization of Swapping Schemes (ZX)	38
4.3 Trusted Node Chain Characterization(ZX, JMc)	40
4.4 Quantum Error Correction Results (JMa)	41
4.5 Performance Analysis of Entanglement Purification Module (JMa)	41
4.6 Performance Analysis of Repeater Chains (All)	43
4.7 Performance Analysis of Quantum Key Distribution (HZ)	47
5 Discussion	52
5.1 Future Modelling Methods Improvements (HZ, ZX, CM, JS, JMa)	52
5.2 Future Work	53
5.3 Conclusions (All)	54
References	57

1 Introduction

1.1 Motivation (JMc)

Quantum communications is a new and rapidly developing field. It has many applications that are already being implemented worldwide. Quantum key distribution (QKD) is one example that is being adopted rapidly in industry to provide quantum-secured communication. Another case is using quantum networks for distributed quantum computation [2].

Due to the field being relatively new, few educational tools exist for undergraduate university students. Those that do exist are back-end focused and require a lot of pre-requisite knowledge. This motivated us to produce a GUI-based program that simulates various simple quantum network architectures in order to give students an intuition for how varying certain physical parameters can effect the performance of a network. The program offers a way to visualise how quantum networks perform under different constraints.

By developing an intuitive GUI-based simulation tool, the entry barrier to understanding the inner-workings of quantum networking is significantly lowered. It provides a means of accelerating learning and potentially research.

1.2 Objectives (JMc)

The project's main objectives are as follows.

1.2.1 Research

In order to gain an in-depth understanding of the field, a significant portion of the project involved reviewing literature in the field of entanglement-based quantum networking. Initially, the most simple network was investigated, a single link involving a mid-point source and two detector nodes. Then, more complicated networks were considered, like the quantum repeater network and the integration of quantum memory. The research is presented in Chapter 2.

1.2.2 Back-end Development and Integration

Using theory from the literature review and further research, simulations were written for each network architecture. This code was then tested to ensure it aligned with currently accepted models and real-world tested networks. Finally, it was linked to the front-end GUI code (Chapter 3).

1.2.3 GUI Development

In order to provide an intuitive simulation tool with a low barrier for entry, an easy-to-use GUI was essential. Other goals of the GUI included, clear and functioning user input, it being able to clearly visualise simulation results and a user-friendly, accessible layout. The way in which the GUI was written and implemented is discussed in Chapter 3.

1.2.4 Testing and Validation

To ensure the simulator produces reliable data, it was important to compare it to currently accepted results. Chapter 4 details these comparisons.

2 Background

2.1 Quantum Link Devices (JS)

Overview: To overcome exponential power attenuation in optical fibre, quantum links and networks leverage entanglement swapping to extend communication distances using quantum repeaters. Entangled photon pairs are probabilistically generated within source devices then transmitted across optical fibre and experience wavelength-dependent attenuation and dispersion. At the receiving node, entanglement can either be immediately measured using a single photon detector or stored using quantum memories for future manipulation or retrieval.

2.1.1 Entangled Photon Pair Sources

Properties of Realistic Sources: Current generation entangled photon pair sources utilize non-linear processes stimulated by a pulsed pump laser to emit entangled photon pairs, such as spontaneous parametric down-conversion (SPDC) or four-wave mixing (SFWM) [3]. A principle drawback of these sources is their nondeterministic emission process. Sources probabilistically emit a random number of pairs per pulse, x . Pair numbers greater than one are generally considered noise and degrade the quality of the source [4]. Sources are characterized by the average number of photon pairs generated per pump pulse, μ . When μ is significantly smaller than the number of temporal modes stimulated by the pump, the probability of emitting x indistinguishable pairs is Poissonian [3]

$$P_{em}(\mu, x) \simeq (1+x) \frac{(\frac{\mu}{2})^2}{(1+\frac{\mu}{2})^{x+2}}. \quad (2.1)$$

Photon Indistinguishability: The pulse pump width affects the quality of emitted photons. Emitted photons have an initial coherence time, $\tau_c = \frac{1}{\Delta v} \approx \frac{\lambda^2}{c\Delta\lambda}$, which is the duration the photon maintains a well-defined phase relationship [5]. If the pump pulse width is significantly larger than τ_c , the pump will generate distinguishable entangled pairs in > 1 temporal mode [5]. Pairs are indistinguishable if all pairs in a multi-pair emission event are generated in the same mode [3].

2.1.2 Optical Fibre

Fibre Selection: After generation from an entangled source, photons are coupled to an optical fibre with an appropriate operating wavelength. Channels in the optical communication band are often selected for minimal attenuation [6]. Quantum wavelength channels have been integrated to coexist with classical ones using dense wavelength-division multiplexing (DWDM), and recent work has demonstrated coexisting quantum and classical channels in the O- and C-bands with as small as 50 [GHz] channel spacings [7]–[9].

Adverse Effects of Fibre Transmission: Photons experience both attenuation and dispersion during transmission. Attenuation rates impose a maximum transmission distance and motivate quantum repeater node placement [10]. As the photon propagates, its temporal envelope broadens due to wavelength-dependent group velocity dispersion. The amount of pulse broadening is governed by $\Delta t = DL\Delta\lambda$, where D is the dispersion parameter [ps / (km nm)], L is the transmission length [km], and $\Delta\lambda$ is the bandwidth [nm] [11]. Both the temporal envelope and τ_c are critical to consider for interfacing network devices. The length of the temporal window contributes to uncertainty in detection time [12]. τ_c restricts interference operations like optical Bell-state measurements, which require two photons to interfere within their mutual coherence time to succeed, which is discussed further in Section 2.2.2 [9].

2.1.3 Single Photon Detectors

Photon Number Resolution: Single photon detectors are categorized by their ability to perform photon number resolution (PNR). Detectors with no PNR will trigger once for any number of incident photons. Detectors with some PNR can be realized by combining multiple non-PNR detectors. PNR detectors output a response proportional to the number of incident photons up to some saturation. PNR is desirable to discern noisy multi-pair detection events [13].

Detector Characteristics: All detectors share a set of physical characteristics [14]. Detectors are optimized to detect photons within a wavelength range, labelled the spectral response. The ratio of detected photons to incident ones is denoted the detection efficiency, η_d . After each detection, there is a certain recovery period where the detector cannot detect any photons, labelled the dead-time. Detectors can inversely trade-off detection efficiency and dead-time. Due to a photon's non-zero temporal window, detection times have some amount of variance, or jitter. Additional jitter arises from certain properties

of the device, such as the type of superconducting material used or electronic readout noise. [14]. Detectors also introduce noise into the system by dark counts, which occur when no photon is incident but a detection is registered. Current work aims to realize PNR detectors capable of high detection efficiency with low jitter and dark counts [13].

2.1.4 Time-Bin Entanglement

Qubits can be encoded in various photonic degrees of freedom, with experimental demonstrations commonly choosing polarization states or time-bins (i.e. early or late photon arrival) [9], [15]. Time-bin qubits benefit from more stable long-distance transmission, as they are less affected by polarization drift and mode dispersion than polarization states. Time-bin qubits are disadvantaged by greater difficulty implementing unitary gates and measurements [15]. Kim [15] demonstrates the generation of time-bin entangled photons in the $|\Phi\rangle$ Bell-state. Two time-delayed pump pulses are generated from a pump laser in the C-band. These pulses undergo second harmonic generation, then perform SPDC to create single signal and idler photons in the C-band. This yields the state

$$|\Phi(\theta)\rangle = |E\rangle_s |E\rangle_i + e^{i\theta} |L\rangle_s |L\rangle_i = |0\rangle_s |0\rangle_i + e^{i\theta} |1\rangle_s |1\rangle_i \quad (2.2)$$

where $\theta = 0$ corresponds to $|\Phi^+\rangle$ and $\theta = \pi$ corresponds to $|\Phi^-\rangle$. To produce $|\Psi\rangle$ at optical wavelengths, Clementi [16] generates SFWM within an integrated silicon photonic chip using a Mach-Zehnder interferometer to control the relative phase between pump signals within two micro-ring resonators to produce

$$|\Psi(\theta)\rangle = |E\rangle_s |L\rangle_i + e^{i\theta} |L\rangle_s |E\rangle_i = |0\rangle_s |1\rangle_i + e^{i\theta} |1\rangle_s |0\rangle_i. \quad (2.3)$$

2.1.5 Entanglement Visibility and Fidelity

Entanglement quality is commonly reported using two-photon interference visibility, which describes multi-pair emissions and other sources of noise in the system. To calculate a system's visibility, the maximum and minimum coincidence count rates of the source must be approximated or measured, R_{max} and R_{min} , respectively [3], [8], [9]. Coincidences are defined as mutual photon detections between both detectors occurring within a configurable time, denoted the coincidence window, τ_{coinc} [17]. A true coincidence event contains only entangled photons from the same pair. Any coincidence containing at least one noisy detection is considered an accidental coincidence [9]. The entanglement visibility and fidelity [3], [9] are then

$$V_{ent} = \frac{R_{max} - R_{min}}{R_{max} + R_{min}}, \quad F_{ent} = \frac{1 + 3V_{ent}}{4}. \quad (2.4)$$

Due to the non-zero probability of noisy pair emission and dark counts, realistic systems have a $R_{min} > 0$ and less than perfect fidelity. As transmission decreases, the effect of multi-pair detection further decreases the source's visibility. Even with no attenuation, multi-pair emission can decrease fidelity due to coincidences between photons from different pairs. Therefore, it is not possible to realize perfect visibility without PNR detectors [3], [9]. However, links utilizing non-PNR detectors have demonstrated Bell-inequality violation, achieving suitable fidelity to support entanglement applications such as quantum teleportation protocols [7]–[9].

2.2 Quantum Repeater Network Structures (ZX, HZ)

Quantum key distribution (QKD) technology plays a crucial role in network security by providing continuous streams of random keys for both parties. However, due to noise and loss in quantum channels, QKD suffers from a strict distance limitation: as reported in [18] and [19], practical systems today struggle to exceed 10 [kbps] at a distance of 50 [km]. This makes it challenging to meet the key rate demands of nationwide networked physical infrastructures using point-to-point QKD alone. Therefore, strategies must be employed to extend the communication distance and increase the key rate. Two commonly discussed solutions are entanglement swapping relays [1], [10], [20]–[23] and trusted node relays [24], [25]. Both approaches divide a long quantum channel into multiple shorter links, thereby increasing the key generation rate on each link and enhancing the overall end-to-end key rate and coverage.

2.2.1 Trusted Node Relay

In a trusted node relay scheme, several trusted intermediate nodes are placed between the communicating parties (Alice and Bob), and each pair of adjacent nodes executes a QKD protocol to establish a shared key. The key generated on the first link

(Alice to the first relay) is termed the service key and is forwarded hop-by-hop until it reaches Bob. This key acts as the session key for OTP encryption. The independently generated keys between relays and their downstream nodes are known as relay keys and are used to encrypt and forward the service key at each hop. Specifically, in each hop, the relay key and service key undergo XOR encryption and are passed to the next link; the downstream node decrypts the message using its relay key and re-encrypts it using the next relay key. This process continues until the service key reaches Bob. The process above can see in the Fig. 3.9. Since the service key appears in plaintext in the memory of each relay node during forwarding, all relay nodes must be fully trusted and physically secured to prevent any third-party access to the keys. A traditional and simple approach to estimating the secret key rate (SKR) over whole link is to approximate the total SKR by the minimum relay key rate across all links:

$$\text{SKR}_{\text{total}} = \min\{\text{SKR}(A, R_1), \text{SKR}(R_1, R_2), \text{SKR}(R_2, R_3), \dots\} \quad [24] \quad (2.5)$$

However, this method overlooks the actual relay-waiting process and its influence of delay on the end-to-end SKR. Due to the randomness inherent in QKD, the key generation rates across different links may vary. Consequently, the service key bits generated by the upstream link may have to wait for relay keys from the downstream link, or vice versa. Without proper coordination, this can lead to delays or even key transmission blockages. In practice, therefore:

$$\text{SKR}_{\text{total}} < \min\{\text{SKR}(A, R_1), \text{SKR}(R_1, R_2), \text{SKR}(R_2, R_3), \dots\} \quad (2.6)$$

To address this, this report adopts a model proposed by Peng-Yong Kong [25], which accurately evaluates the end-to-end key rate in multi-relay scenarios and, for the first time, incorporates the randomness and buffer waiting effects of relay operations. The model identifies the necessary conditions for stable relay operation and provides a theoretical formula for SKR calculation. By using this model, the performance comparison of Kong's model and traditional model of SKR and relevant parameter analysis will be demonstrated in Section 4.3

2.2.2 Entanglement Swapping Relay

This architecture is specifically designed for entanglement-based QKD protocols such as E91 and BBM92, and is not applicable to BB84. Its purpose is to establish a series of entangled photon pairs between Alice and Bob. The typical components include entangled photon pair sources (time-bin encoding is used in this case), quantum memory, linear optical Bell state measurement (BSM), single-photon detectors, and optical fibre. The structure of the entanglement swapping node is not fixed; it can be categorized as either Memoryless Swapping or Memory-Based Swapping [26], depending on the presence of quantum memory. It can also be classified as Sequential [22], Doubling Tree [1], [10], Parallel [21], or Opportunistic [20], [23] based on the order in which relay BSMs are executed. See Fig. 3.8 for more detail. Among these, The Doubling Tree scheme is one of the most widely studied: its swapping operations follow a balanced binary tree structure of height $\log_2(N)$, and nodes at the same level can perform swapping in parallel. It supports hybrid use of memory and memoryless operations. For example, in the Guha architecture [1], which we will focus on later, the first-layer relay operations are defined as memoryless, requiring simultaneous and successful BSMs—similar to the Parallel scheme which leads to a very low success probability:

$$P_{\text{total}} = \eta_{tr}^N, \quad \eta_{tr} = 10^{-\frac{\alpha L}{10}} \quad (2.7)$$

where η_{tr} is the fibre loss in each link. N is the number of single links, α is the fibre attenuation coefficient in dB/km, and L is the fibre length for each segment in km. To overcome the low success probability in this scheme, WDM is proposed to increase η_{tr} . If M frequency-multiplexed entangled pairs are used, then:

$$\eta_W = 1 - (1 - \eta_{tr})^M. \quad (2.8)$$

This significantly enhances link performance and mitigates the limitations of memoryless swapping, but it requires more advanced hardware control and increases system complexity and cost. Thus, it involves a trade-off. Further analyse this architecture and evaluate its performance is showed in Section 3.3.

2.3 Quantum Optical Memory (CM)

In this paper, quantum memories (QM) refer to devices designed to store photonic qubits, including entangled photons [27]. They enable buffering and re-timing of quantum information. As such, they play a crucial role in extending the maximum distance of quantum communication channels as components of quantum repeaters [28], which is essential for this simulator. This section discusses quantum memories for storing single photons in entanglement-based communication. In general, quantum memories can be classified into three categories: non-atomic memories (NAMs), linear atomic memories (LAMs), and non-linear atomic memories (NLAMs).

NAMs are currently still largely experimental and are less suitable for quantum communication due to their reliance on mechanical systems. This results in high noise and short coherence times [29]. NLAMs require strong photon–photon interactions to induce non-linear effects, which remain technically challenging to achieve at the single-photon level. Consequently, current implementations tend to have relatively low efficiency despite the promise of deterministic operation [27].

Therefore, this paper will mainly focus on Λ -type LAMs, which are among the most experimentally developed quantum memory systems due to their high efficiencies, on-demand readouts, and compatibility with entangled photons. The various protocols and platforms for implementing LAMs are discussed in Sections 2.3.2 and 2.3.3, respectively.

2.3.1 Basic Concepts (CM)

The general objective of a quantum memory is to map flying qubits onto a collective atomic state [28]. A generic model of a Λ -type atomic medium consists of an excited state $|e\rangle$ optically coupled to a ground state $|g\rangle$ and a metastable state $|s\rangle$, as shown in Figure 2.1. The input (probe) field couples $|g\rangle \leftrightarrow |e\rangle$, creating a collective optical coherence (atomic polarisation) between these states, with detuning Δ . A classical control field with time-dependent Rabi frequency $\Omega(t)$ couples $|s\rangle \leftrightarrow |e\rangle$ with the same detuning Δ , coherently transferring the excitation into a spin wave, a long-lived collective coherence between $|g\rangle$ and $|s\rangle$ in which the photonic information is stored [28], [30]. The detuning Δ is the frequency difference between the $|g\rangle \leftrightarrow |e\rangle$ transition and the probe field: $\Delta = \omega_{eg} - \omega_{\text{probe}}$. A more detailed mathematical explanation is provided in Section 3.5.

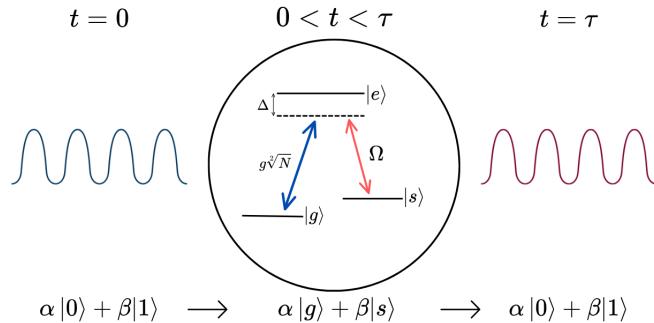


Figure 2.1: Illustration of quantum information storage and retrieval in a Λ -type atomic memory with storage time τ . The probe field (blue arrow) couples the ground state $|g\rangle$ to the excited state $|e\rangle$ with effective coupling $g\sqrt{N}$ and detuning Δ , where N is the number of atoms. A classical control field (red arrow) with Rabi frequency Ω couples the metastable state $|s\rangle$ to $|e\rangle$, also with detuning Δ .

2.3.2 Protocols (CM)

LAMs can be broadly categorised into two types: absorptive and emissive memories. The absorptive protocols covered in this paper include electromagnetically induced transparency (EIT), off-resonant Raman, Gradient Echo Memory (GEM), and atomic frequency comb (AFC). The emissive protocol is not discussed as it is irrelevant to the simulation in this paper.

Optically Controlled Memories: Both electromagnetically induced transparency (EIT) and off-resonant Raman scattering are optically controlled memories with similar storage and retrieval mechanisms, as both use a control field to reversibly map flying qubits onto atomic states. By gradually switching the control field on or off, photonic information is adiabatically transferred to or from a spin-wave. Moreover, these protocols do not require an inhomogeneously broadened absorption line. As shown in Section 3.5, both protocols can theoretically achieve the same maximum efficiency [30], though there are important differences between them.

EIT operates in the resonant limit ($\Delta \rightarrow 0$), where an otherwise opaque atomic medium becomes transparent at the probe frequency. In this regime, the probe field experiences a reduced group velocity inside the medium. Storage is achieved by progressively turning off the control field to map the probe into the spin-wave, while retrieval is done by turning it back on [28], [30].

In contrast, the off-resonant Raman protocol uses both control and probe fields far detuned from state $|e\rangle$. Like EIT, it relies on adiabatic transfer of photonic information to the spin-wave via the control field, but storage is mediated by Raman scattering. The large detuning requires a stronger control field than EIT [28]. The multimode capacity of both protocols scales as \sqrt{d} , where d is the optical depth [31]. Raman memories, however, support higher capacity since large detuning broadens the acceptance bandwidth, enabling shorter pulses and more temporal modes [30]. By contrast, EIT relies on spatial compression of photons within the narrow medium, which severely constrains capacity [27].

Engineered Absorption Memories: Both gradient echo memory (GEM) and atomic frequency comb (AFC) are engineered absorption protocols, typically implemented in rare-earth (RE) ion-doped solids due to their broad inhomogeneous absorption lines.

In GEM, a narrow absorption feature is first prepared by optical pumping [28]. An external electric or magnetic field then detunes the ions linearly along the medium, broadening the feature. When a probe pulse enters, it is collectively absorbed by the ensemble. Retrieval is achieved by reversing the field, which rephases the ions and produces a coherent echo of the input field. This protocol enables fully on-demand recall, limited by the optical coherence time (or spin coherence time in a Λ -system) [32], and is highly efficient due to suppression of re-absorption [28].

In AFC, the inhomogeneous line is spectrally tailored into a periodic comb of narrow absorption peaks with spacing Δ . When a probe is absorbed, the comb teeth accumulate phases that re-align after a fixed delay $t_{\text{fix}} = 1/\Delta$, producing a photon echo without external control [33]. Thus, AFC alone is not on-demand, but transferring the excitation to a spin state with a control field extends storage well beyond t_{fix} and allows on-demand retrieval.

Both protocols offer high multimode capacity owing to inhomogeneous broadening. In GEM, capacity scales linearly with optical depth [28], while in AFC it is independent of optical depth and instead determined by physical parameters [33].

2.3.3 Platforms (CM)

Several physical media are suitable for quantum memory protocols. Two notable platforms are rare-earth (RE) ion-doped solids and alkali vapours. These platforms are chosen because they have been demonstrated to operate effectively with the protocols discussed, offering complementary advantages such as in efficiency and storage time.

RE ion-doped solids exhibit very narrow homogeneous linewidths and long optical and spin coherence times at cryogenic temperatures. Their large inhomogeneous broadening can be spectrally tailored by optical pumping, enabling protocols such as AFC and GEM with high multimode capacity and efficient storage of time-bin entangled qubits [27], [32]. These properties make them attractive for long-lived storage, though they require cryogenic cooling and most operate outside the telecom band.

Alkali vapours naturally provide high resonant optical depth at near-infrared wavelengths when operated at "warm" temperatures (50–100°C), without the need for cryogenics. They possess spin states that suppress fluorescence noise and support long coherence times, making them well-suited for Λ -type protocols such as EIT and Raman [27]. However, coherence is ultimately limited by Doppler broadening and atomic motion.

2.3.4 Noise Sources (CM)

There are several sources of noise in quantum memories. First, control field leakage via imperfect spatial separation or scattering can enter the detection mode. This requires careful filtering. This leakage is common to all Λ -type, control-pulse-based quantum memories [27]. Second, fluorescence noise occurs when atoms are excited to the state $|e\rangle$ and then decay spontaneously, producing incoherent photons. This results in loss of fidelity and signal contamination. Protocols with small detuning, such as EIT and AFC, are more susceptible to incoherent fluorescent emission [27], [34]. Finally, four-wave mixing (FWM) noise can occur when the intense control field drives nonlinear interactions in the medium, generating unwanted photons in the detection mode. Raman memories, which use relatively stronger control fields, are more prone to FWM compared to EIT [27], [30].

2.3.5 Figures of Merit and Recent Advances (CM)

Key figures of merit for assessing quantum memories include fidelity, efficiency, bandwidth, storage time, operating wavelength, and multimode capacity. Fidelity measures the overlap between the retrieved and input quantum states [28] and can be

expressed as $F_{\text{retrieved}} = F_{\text{memory}} \times F_{\text{input}}$. Efficiency quantifies the probability of successfully storing and retrieving a photon, and depends on both the protocol and physical parameters. Bandwidth defines the optical frequency range over which the memory can operate efficiently. A broader bandwidth $\Delta\omega$ allows shorter pulses $\tau \approx 1/\Delta\omega$, allowing higher repetition rates and larger multimode capacity [28]. Storage time, determined by the coherence time of the platform, must at least match the entanglement generation time, and on the order of milliseconds is typically required to extend beyond the distance limit of direct transmission [27], [28]. Wavelength is largely influenced by the choice of protocol and medium. Finally, multimode capacity refers to the number of distinct quantum states that can be stored at the same time in a single memory, with higher capacities leading to increased communication rates [28].

Table 2.1 summarises key figures of merit from state-of-the-art quantum memory experiments. These values serve as the default parameters in the simulator. All listed memories are compatible with time-bin entanglement, which is relevant to this work.

	Hot Rb Vapour^a	Hot Rb Vapour^b	RE crystal (Er³⁺)^a	RE crystal (Eu³⁺)^a	RE crystal (Pr³⁺)^a
Protocol	EIT	Far-off Raman	AFC	AFC	GEM
F	0.97	0.98	0.98	>0.95	0.98
η_{gm}	0.67	0.82	0.22	0.1	0.69
τ_s	100ns	1.1μs	660ns	21μs, 1h	1.2ms
$\Delta\omega$ (MHz)	<1	100	6	700, 1	0.14
T (K)	368	351.7	1.5	3.5, 1.7	3
B (T)	0	0	7	0, 1.3	0
λ (nm)	795	795	1536	580	606
MC	-	60	1650	>100	10^5 (est.)

Table 2.1: Summary of key figures of merit from recent stand-alone quantum memory experiments across various protocols and platforms. The table lists fidelity (F), efficiency (η), storage time (τ_s), bandwidth ($\Delta\omega$), operating temperature (T), applied magnetic field (B), wavelength (λ) and multimode capacity (MC). References a : [28], b : [35].

2.3.6 Discussion (CM)

The choice of memory protocol and platform strongly affects performance and integrability, with trade-offs summarised in Table 2.1. Beyond fidelity and efficiency, parameters such as bandwidth and multimode capacity are also critical for maximising communication rates. For example, EIT, though experimentally mature, is severely limited in multimode capacity [27]. Integration into multiplexed systems would therefore require many parallel memories, reducing practicality and overall success probability. Raman protocols demand stronger control fields and suppression of FWM noise but provide broader bandwidths, enabling shorter pulses and higher entanglement rates. By contrast, GEM and AFC support far higher capacities and communication rates, but typically require cryogenic operation. In addition, most platforms (e.g. Rb- or Eu-based) operate outside the telecom band, necessitating quantum frequency conversion, which further reduces efficiency. Lastly, since this simulator is designed for long-distance communication, fidelity, efficiency, and storage time remain the most critical parameters, while others are provided for users to evaluate according to their needs.

2.4 Quantum Frequency Converter (CM)

Table 2.1 highlights that most quantum memories operate outside the telecom band, making a quantum frequency converter (QFC) essential as an interface to telecom networks. Waveguide-based QFC devices (QFCDs) using difference-frequency generation have been demonstrated for Rb-based [36] and Pr-based [37] quantum memories. Although the memories in these works are emissive, the QFCD is compatible with our system since the heralding signal from the emissive memory can be replaced by the heralding click from the BSM inside the repeater node. Moreover, the Pr-based demonstration further suggests that QFC integration is feasible for the Eu-based memory [37]. The QFCD achieved maximum device efficiencies of 13.6% (Rb-based) and 24.5% (Pr-based). In the Rb-based case [36], the total efficiency of the combined memory–QFC system is $\eta_R = \eta_{\text{memory}} \eta_{\text{trans}} \eta_{\text{qfcd}}$, where $\eta_{\text{trans}} = 0.77$ is the transmission efficiency from the memory to the QFC. The maximum fidelity of this integrated memory–QFC structure is $F \leq 0.94$.

2.5 Quantum Error Mitigation Strategies (JMa)

Long-distance entanglement distribution is limited by fiber loss, detector dark counts, multi-pair emissions from probabilistic sources, and memory decoherence. In our repeater models we therefore combine two complementary approaches: *quantum error correction* (QEC), which actively repairs errors in a one-way, pipeline fashion, and *entanglement purification* (EP), which probabilistically upgrades fidelity using LOCC before entanglement swapping. QEC removes two-way latency but demands substantial hardware overhead and high-fidelity control; EPP is hardware-lighter and robust to moderate gate noise but incurs rate loss from heralding and the linear-optical Bell-state-measurement (BSM) limit. These trade-offs are consistent with standard repeater “generations” [38]–[41].

2.5.1 Quantum Error Correction (QEC)

QEC encodes one logical qubit into many physical qubits so that *syndrome* measurements identify and correct errors without revealing the logical state [42], [43]. A code of distance d corrects up to $t = \lfloor (d - 1)/2 \rfloor$ arbitrary single-qubit errors; below threshold, concatenation or topological codes suppress logical error roughly exponentially with d [44]. For communication, erasure-/loss-tolerant stabilizer encodings enable *one-way* repeaters that correct errors at intermediate nodes instead of discarding pairs, eliminating round-trip latency and boosting achievable rates once gates, measurements, and memories are sufficiently reliable [40], [41], [45]. The bottleneck shifts to resources (qubit count per logical link, high-fidelity/low-latency control), but the scaling advantage is substantial when thresholds are met [40], [44].

2.5.2 Entanglement Purification (EPP)

EPP consumes multiple noisy Bell pairs to probabilistically output fewer, higher-fidelity pairs via LOCC (e.g., BBPSSW / DEJMPS) provided the input (e.g., Werner) fidelity exceeds $1/2$ [46], [47]. In repeater chains, neighboring nodes store several raw pairs in memories, run recurrence or pumping steps, and keep heralded outputs with $F' > F$ before swapping [38], [39]. Linear-optical BSMs can unambiguously identify at most two of four Bell states, capping per-attempt success at $\leq 1/2$ even with ideal detectors [48]; spectral/spatial multiplexing with M modes mitigates this via an effective success $1 - (1 - p)^M$. EPP therefore trades *rate for quality* and requires memories coherent over classical round-trip times, but is well matched to today’s probabilistic photonic links [39], [41], [49].

2.6 GUI Development (JMc)

2.6.1 Goals

The motivation behind the project was to develop an easy-to-use, intuitive GUI-based program for simulating quantum networks. The program is specifically designed for educational purposes at the university level to provide intuition on how changing network parameters effects quantum network performance. Implementing a straight forward GUI is essential for educational purposes in order to avoid confusion and unnecessary complexities. Below is the product design specification that has been adhered to.

Product Design Specification

- **Purpose:** The purpose of the GUI is to provide an accessible and intuitive interface for running and visualizing quantum network simulations. The GUI allows users to define network parameters, run simulations through the back-end code, and analyse results via graphs and metrics.
- **Scope:**
 - **GUI scope:**
 - * GUI can handle user input that specifies network architecture and parameters.
 - * Links to the back-end to execute quantum network simulation code.
 - * Returns easy to interpret graphs and data that is produced by the back-end simulation code.
 - * User can save data after running the simulation.
 - **Back-end scope:**
 - * Implementation of quantum network simulations

- * Returning data in the form a graphs
- **User experience**
 - **Primary users:** Students, researchers.
 - **Secondary users:** Teachers/educators when demonstrating concepts.
- **Functional Requirements**
 - **Input handling**
 - * User is able to select their desired network preset architecture.
 - * User can input the physical parameters for each component e.g source repetition rate.
 - * The program can validate inputs and ensure they are physically meaningful and won't cause simulation errors.
 - **Simulation control:** The user can start, pause and stop a simulation with ease.
 - **Visualisation:** Data can be visualised in an easy-to-interpret manner (in this case plots of data).
 - **Data management:** The user has the option to save the raw data produced by the simulation.
- **Non-functional Requirements**
 - **Usability:** The GUI is intuitive and easy to learn to navigate.
 - **Performance:** The software is written in an efficient manner to maximise performance.
 - **Reliability:** The software runs consistently without running into problems that may crash the program.
- **Design Constraints**
 - The software is implemented using python,
 - The GUI is implemented using open source frameworks e.g Qt for python, matplotlib.

An initial wireframe design of the GUI was produced to assist in the actual design. The sketch shows the basic layout desired for the GUI. It features a "drawing area" where the network architecture is displayed to the user. Furthermore the sketch indicates where the components of the network are displayed and where the user can adjust the network's parameters. It also shows where the results are displayed. This is shown in figure 2.2.

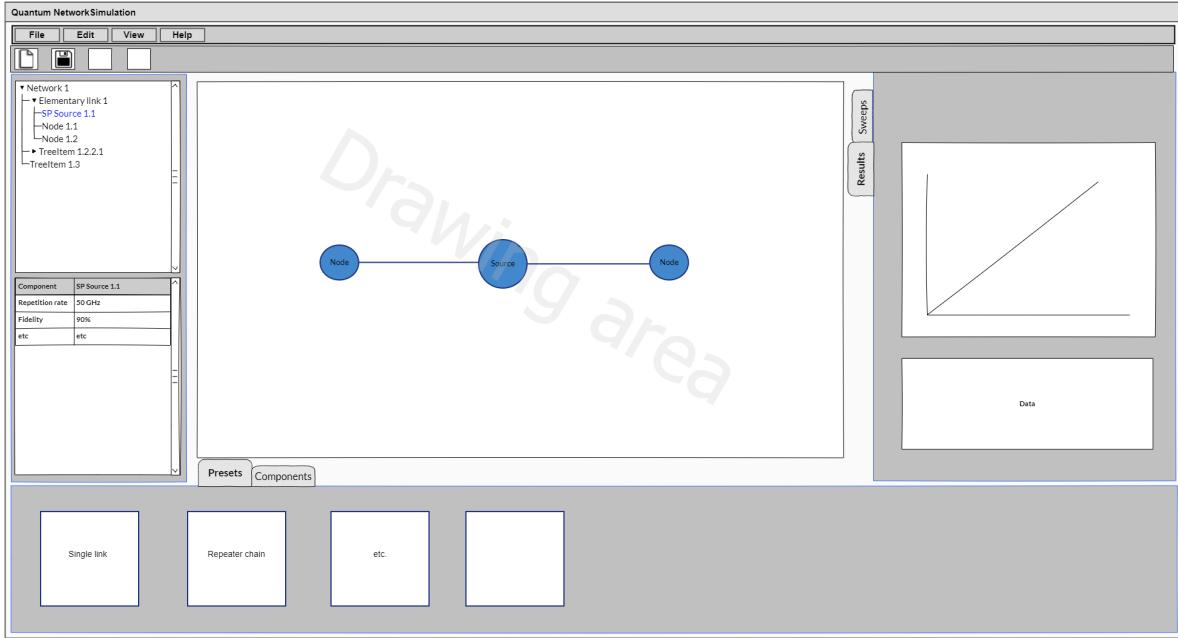


Figure 2.2: Initial plan of GUI layout

This wireframe design has evolved throughout the development process and the final outcome of the GUI design is shown in chapter 3.

2.6.2 Qt Framework

The Qt framework [50] is a widely used development tool for creating GUIs. It was selected for developing the simulation software due to its extensive documentation and support available. Specifically, the python binding of Qt was used. This was chosen due to its simplicity compared to the original language c++. The developers of the Qt framework also offer a free student license for their software "Qt Creator". Qt Creator makes GUI development much easier as it provides a visual approach as opposed to a purely code-based method. Once developed, back-end functionality was added to the GUI. This is detailed in chapter 3.

3 Methods

3.1 Software Structure and Implementation (JMc)

The core of the simulation is based on the Qt framework. Figure 3.1 shows a high level block diagram illustrating the structure of the program and how the GUI class app.py connects to the back-end simulation classes. This is not an exhaustive list of the simulation classes used. The code is available for further review [51].

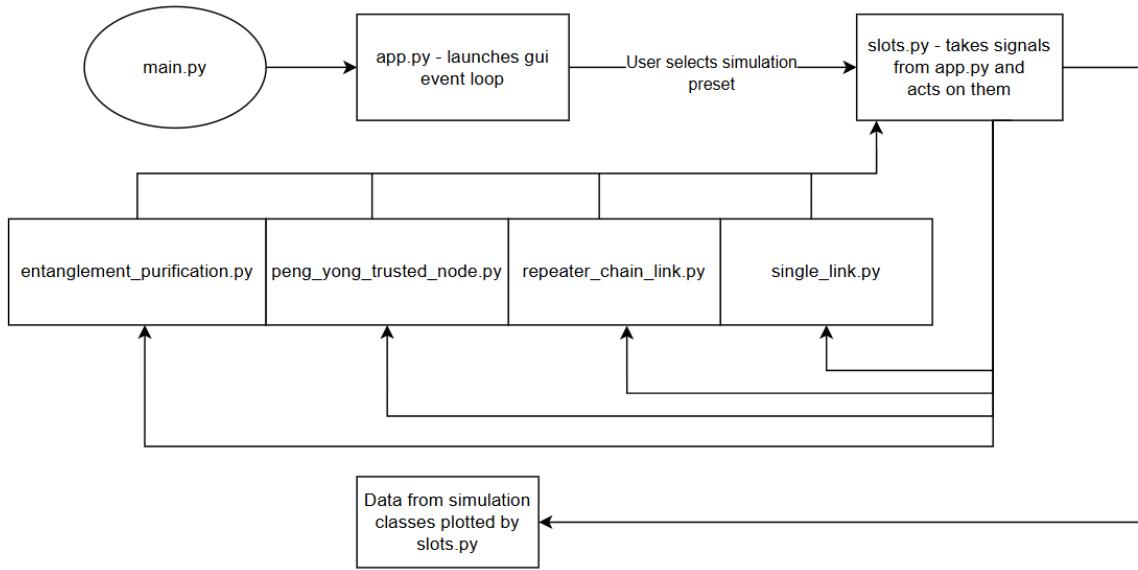


Figure 3.1: High level block diagram showing how the GUI interacts with simulation classes

The file main.py is run and this calls app.py which initialises the GUI and launches the program. app.py contains code that reacts to what Qt call a "signal". This is an action from the user such as clicking a button. The file slots.py contains all the actions that are performed when a signal is sent. "Slots" is the name given to these actions.

All back-end components of the program are stored separately. They consist of python classes that are instantiated in the slots.py file. When the user selects a simulation to run, the app.py file sends the data to the slots.py file. The slots.py file then calls the appropriate back-end class to run. Once complete, the simulation results are displayed by the slots.py file. slots.py is essentially the central nervous system of the program, as it controls all other parts.

The GUI-based program consists of six presets that implement different types of quantum networks. Each network takes parameters for its components and outputs data relating to the network's performance. The network structure and mathematical description of each preset are discussed later in this chapter. Additionally, the software has the ability to sweep over certain network parameters which can be used to estimate the optimum network setup.

The basic event loop of the program is shown in figure 3.2. The user first selects which network architecture they would like to simulate. The user is then shown the list of components in the network in a tree widget. By selecting each component the user has the option to adjust the physical parameters of each component. Subsequently, the user must press "Run". A dialogue box is then displayed to the user that displays the various options required for the simulation to run. This includes a list of independent variables and dependent variables that the simulator can sweep over to test how the network performs under certain conditions. This can be used to find optimal performance parameters. As long as all input data is valid, the program will then return a plot of the data produced during the sweep.

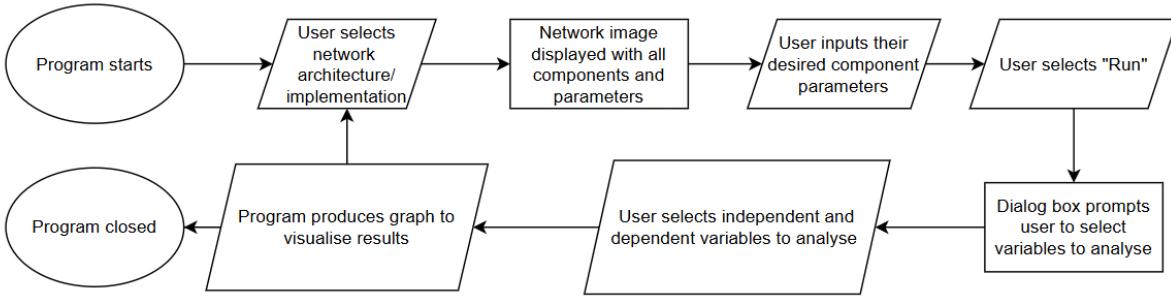


Figure 3.2: Program event loop

3.1.1 Single Link Example

As an example, this section shows how a single link network can be simulated. In particular a single like with an entangled photon source in the middle of the link.

Once the program is open, the user selects "Single Link (Midpoint source)" from the preset tab. The list of components in the network is then displayed on the left. These include the source, and two detectors.

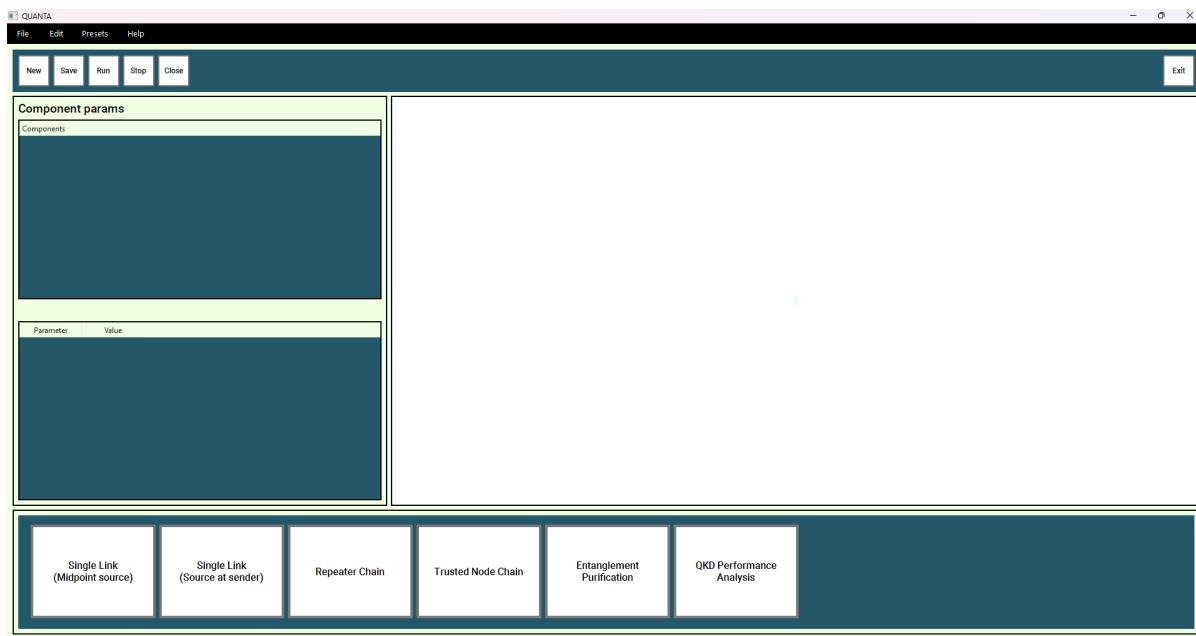


Figure 3.3: Main GUI workspace.

Selecting a component will display its parameters in a table below the component tree. These parameters can be edited by the user (figure 3.4).

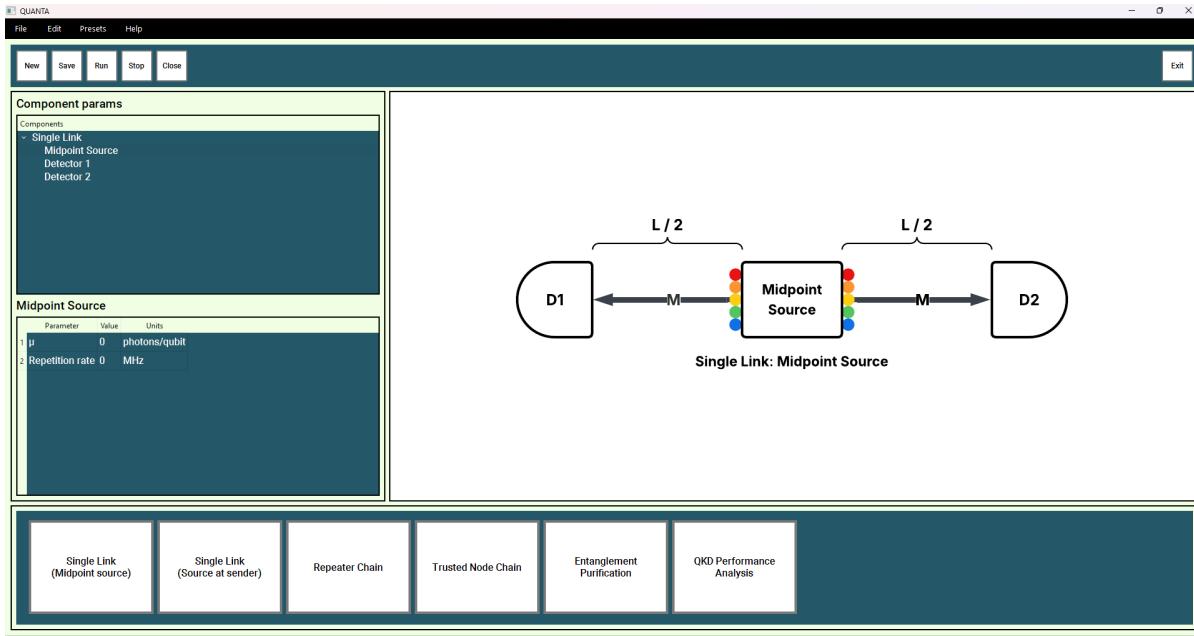


Figure 3.4: Single link (Midpoint source) network open with a list of components and their parameters.

Once all parameters have been entered, the user then clicks the run button in the toolbar.

A dialog box then prompts the user to select the independent and dependent variables they would like to plot. Values for α (fibre attenuation) and the number of data points are also required from the user.

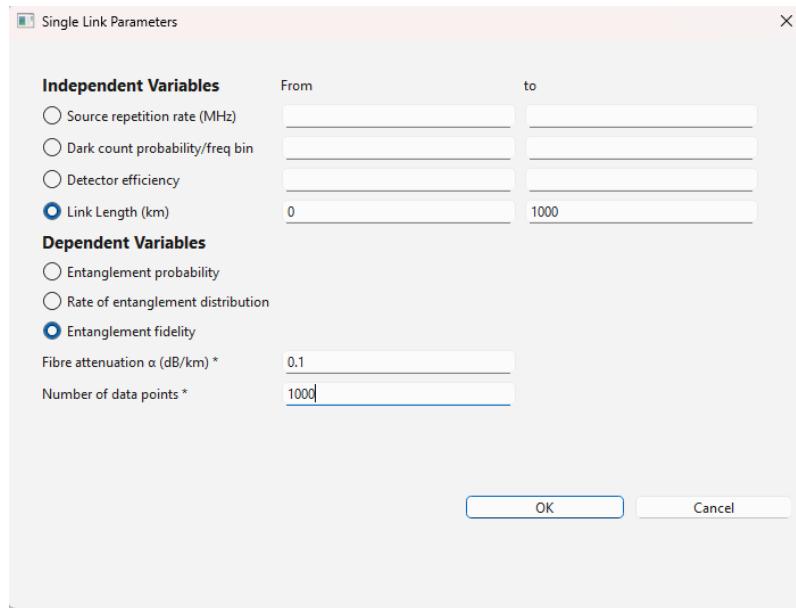


Figure 3.5: Single link simulation dialog box.

The user then clicks "OK" and the simulation will run. Using the matplotlib [52] library, the data is plotted in a new window.

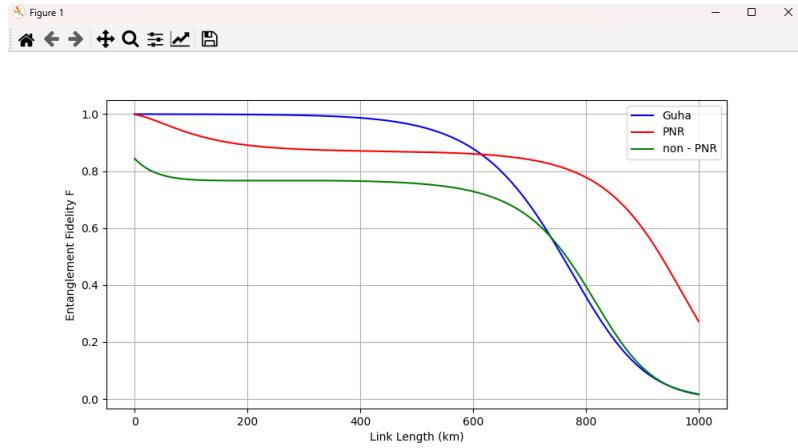


Figure 3.6: Entanglement fidelity vs Link length plotted by the simulator

The methods and theory used for the back-end simulation code are described further in this chapter.

3.2 Single Link Modelling (JS, CM)

3.2.1 System Assumptions

Analytical Modelling Overview: The simulator supports two entanglement distribution link architectures as defined by Beukers [53]: Source-in-Midpoint and Sender-Receiver. Guha [1] present an analytical model for an arbitrarily long quantum repeater chain using Source-in-Midpoint links. The simulator utilizes their repeater architecture and analytical models as a baseline architecture to simulate repeater chain performance. Corresponding equations are derived for each type of single link architecture. Notably, the only source of noise analytically modelled by Guha [1] is detector dark counts, and the effect of probabilistic multi-pair emission on the probability of entanglement distribution per pulse (P_{ent}) and fidelity (F_{ent}) are not considered. Therefore, this section describes the extensions made to model realistic emission processes as function of μ .

A Perfect Link: A deterministic and noise-less Source-in-Midpoint link would contain a source that only emits single photon pairs on-demand, two identical optical fibre with no sources of noise at the quantum wavelength, and a detector with no dark counts [3]. The dead-time of the detector must be shorter than the source's pump repetition period to ensure pulses always arrive when the detector is ready to receive [14]. With these assumptions, τ_{coinc} must be selected to be larger than the detection jitter, which is mainly characterized by τ_c and fibre dispersion [17]. Since all detections are entangled photons from the same pair, τ_{coinc} must encompass all detections. The resulting visibility is unity.

Simulated Sources: To capture the limitations of realistic sources, the simulator models probabilistic sources inspired by Takasue [3], which emit x pairs each with the probability $P_{em}(\mu, x)$ from a Gaussian pump with a repetition rate of R_{rep} [MHz] [54]. The source generates indistinguishable pairs of time-bin entangled photons encoded in the state $|\Psi^\pm\rangle = |E\rangle_s |L\rangle_i \pm |L\rangle_s |E\rangle_i = |0\rangle_s |1\rangle_i \pm |1\rangle_s |0\rangle_i$.

Simulated Links: Photon transmission efficiency across a fibre of length L is modeled by $\eta_{tr} = 10^{-\frac{\alpha L}{10}}$, where $\alpha(\lambda)$ is the attenuation rate [dB/km] at wavelength λ [1]. Each link has access to coarse or dense wavelength-division multiplexing (CWDM, DWDM) devices to support the corresponding number of ITU channels for each technology [55]–[57]. Coexisting quantum channels are assumed to utilize a low launch power such that non-linear process do not occur during transmission and noise photons are not generated at copropagating channel wavelengths. Time-bin entangled photons are minimally affected by polarisation mode dispersion and polarisation dependent loss, therefore these effects are not considered [15]. The two link architecture models differ only in their fibre transmission [53]. A Source-in-Midpoint generates entangled pairs and transmits half of the photons on separate fibre to each node, such that each fibre's transmission is $\eta_{tr} = 10^{-\frac{\alpha L}{10}}$ and $P_{ent} \propto \eta_{tr}^2$. When the source is located within one node in the Source-Receiver configuration, only one photon must undergo transmission across one longer fibre, so $\eta_{tr} = 10^{-\frac{\alpha L}{10}}$ and $P_{ent} \propto \eta_{tr}$.

Simulated Detectors: The simulator models parameters characteristic of free-running single photon detectors [13], [17]. The detection efficiency η_d is combined with η_{tr} to yield the total link efficiency from emission to detection $\eta = \eta_{tr} \eta_d$. We

assume $1/R_{rep}$ is larger than the detector's dead-time. The fibre dispersion is assumed to be characterized, and R_{rep} is chosen such that no pulse overlap from dispersion occurs during transmission. Therefore the temporal window of the arriving photon is known. The detection jitter is assumed to be well characterized, and the coincidence window is chosen to encompass the entire jitter distribution. To account for multi-pair emission and dark count noise, the probability of detecting an accidental coincidence is analytically modelled for non-PNR and perfect PNR detectors. With these assumptions, all true and accidental coincidence detections are modelled.

Simulated QM: In this simulator, quantum memories are assumed to store the full photon rate generated by the source, without explicitly modelling bandwidth or multimode capacity. This simplification is reasonable since the focus is on long-distance communication rather than local processing, making storage time the critical factor [27]. Moreover, spontaneous decay processes of both polarisation and spin-wave modes are not included in the calculation. Instead, the qubit is assumed irrecoverable once the idle time exceeds the storage capability. The efficiencies of loading and retrieval are approximated as $\eta_{gm,tot} = \eta_{read}\eta_{write}$. Lastly, time-dependent noise can be applied as a function of the qubit's idle time.

3.2.2 Guha's Modelling Methods

Single Link Architecture: From the full repeater architecture of Guha [1], the probability of entanglement distribution and entanglement fidelity is derived for a single link connecting two nodes. Entanglement distribution is confirmed, or heralded, when both detectors register a correct coincidence pattern. For the state $|\Psi^\pm\rangle$, heralding is defined as a coincidence in unmatched time-bin modes. If there are no sources of noise in the system, a heralding event always indicates the pure state $|\Psi^\pm\rangle$ was distributed between the two nodes. However, noisy detections from dark counts and unpaired photons create false positive heralding events, lowering the fidelity of entanglement. The probability of entanglement distribution is then $P_{ent} = P_T + P_F$, where the probability of a successful entanglement distribution is P_T and a false positive herald is P_F . Therefore, the rate of entanglement distribution is $R_{ent} = P_{ent}R_{rep}$, and the fidelity of entanglement distribution is $F_{ent} = \frac{P_T}{P_{ent}}$ [1].

Single Link Modelling: Guha [1] define these probabilities for deterministic source only emitting single pairs and non-PNR detectors. The probability a detector clicks per pulse for each time-bin is $P_{click} = \eta + P_{DC}(1 - \eta)$, where P_{DC} is the probability of a dark count per time-bin [1]. Guha define P_T as any herald from only an entangled pair or only dark counts. P_F comprises all other combinations of coincidences in the correct heralding pattern

$$P_T = P_{click}^2(1 - P_{DC})^2 + P_{DC}^2(1 - P_{click})^2, \quad P_F = 2P_{click}P_{DC}(1 - P_{click})(1 - P_{DC}). \quad (3.1)$$

3.2.3 Modelling Extensions to Simulate Realistic Devices

Guha Extensions: Guha's [1] analysis is extended to characterize the effects of probabilistic multi-pair emission. The definition of P_T is updated to only include heralds from entangled photons. Quantum communication protocols leveraging entanglement require quantum correlations and therefore correlations from classical noise are not suitable [58]. Within Guha's analysis, this is updated by setting $P_{T-click} = \eta$ and moving the symmetrical dark count herald to P_F

$$P_T = P_{T-click}^2(1 - P_{DC})^2, \quad P_F = P_{DC}^2(1 - P_{click})^2 + 2P_{click}P_{DC}(1 - P_{click})(1 - P_{DC}). \quad (3.2)$$

PNR Detectors: Clark [4] describes P_T and P_F using PNR detectors, where the probability of detecting n photons from x pairs is $\binom{x}{n}\eta^n(1 - \eta)^{x-n}$, and $\binom{x}{n}$ is the binomial coefficient. PNR detectors can identify detection events where $n > 1$, which are omitted from coincidence counts. True heralds only occur when one photon is detected per node, so only coincidences from single unpaired photons are false herald events. For indistinguishable photons, this corresponds to M combinations of detection events, where true heralds have $M_T = \binom{x}{1} = x$ combinations, and false ones have $M_F = \binom{x}{2} = \frac{x(x-1)}{2}$ combinations from broken pairs. Assuming both fibres and detectors have equal η in a Source-in-Midpoint link¹, the probabilities of true and false heralds with PNR detectors are

$$P_{i=T,F} = \sum_{x=0}^{\infty} P_{em}(\mu, x) M_i \eta^2 (1 - \eta)^{2(x-1)} \quad (3.3)$$

To include dark counts, Clark's analysis [4] is extended to include true and false heralds from dark counts in the same format

¹Each component's unique efficiency can be configured in the simulator.

as Guha's Eq. 3.2.

$$P_{TDC} = \sum_{x=0}^{\infty} P_{em}(\mu, x) M_T \eta^2 (1-\eta)^{2(x-1)} (1-P_{DC})^2 \quad (3.4)$$

$$P_{FDC} = \sum_{x=0}^{\infty} \left[P_{em}(\mu, x) M_F \eta^2 (1-\eta)^{2(x-1)} (1-P_{DC})^2 + P_{em}(\mu, x) \binom{x}{1} \eta (1-\eta)^{2x-1} P_{DC} (1-P_{DC})^2 + 2P_{em}(\mu, x) (1-\eta)^{2x} P_{DC}^2 (1-P_{DC})^2 \right] \quad (3.5)$$

The second summation term of P_{FDC} defines heralds in which a single photon reaches one node and all photons are lost at the other, which is replaced by a dark count. The third considers a herald where all photons are lost and only dark counts produce the heralding pattern in either two sets of unmatched bins.

Non-PNR Detectors: This can be extended to model non-PNR detectors. By definition, P_T does not change, and P_F must be adapted to consider all correct detection patterns as potential heralds. The detector cannot omit events with more than one detected photon and clicks with probability $P_{click} = (1 - (1-\eta)^x) + P_{DC}(1-\eta)^x$. Mirroring Guha's Eq. 3.2, P_{ent} becomes

$$P_{ent} = \sum_{x=0}^{\infty} P_{em}(\mu, x) P_{click}^2 (1-P_{DC})^2 \quad (3.6)$$

Quantum Memory: As discussed in Table 2.1, experimental demonstrations of QM often report the total QM η , which is related to the loading and emission efficiencies. To store the entangled photons in QM rather than detect, the non-PNR equations can be adapted, as only one photon can be stored in each QM position (Section 3.2.1). η is updated in Eq. 3.6 to be $\eta = \eta_{tr}\eta_{write}$ and P_{DC} is removed.

3.3 Quantum Repeater Chain (ZX, JS)

3.3.1 Guha's Architecture (ZX, JS)

Guha's repeater chain structure [1] is used as the foundation for this study of entanglement-swapping-based quantum networks. In this structure, each elementary link node (orange) performs a BSM as the first-layer swapping unit, analogous to the first

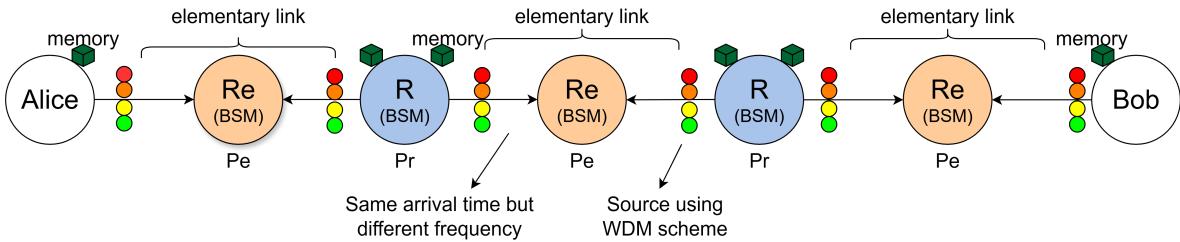


Figure 3.7: Guha's repeater chain structure

level of execution in a binary tree structure. Fig 3.7 illustrates Guha's repeater chain architecture, where the number of elementary links $N_e = 3$. The success probability of each elementary link is indicated as P_e , where P_e includes fiber loss η_{tr} and the BSM success probability $P_b < 0.5$, which is affected by detector efficiency η_d and the choice of the width of the coincidence time window. The success probability of each repeater node (blue) is P_r , where P_r includes the P_b of the repeater node, which not only affected by detector efficiency η_d but also memory efficiency η_m . Therefore, the total link success probability is given by the following formula:

$$P_{succ} = P_e^{N_e} \cdot P_r^{N_e-1} \quad (3.7)$$

Where N_e equals the number of elementary links. According to this formula, Guha's raw key rate equation is defined as

$$R_{raw} = P_{succ} \cdot \frac{1}{T_q} \quad (3.8)$$

this equation come from Equation(1) of [1] (ignore those sift process). where T_q represents the source period. However, this equation is not perfect nor comprehensive because it does not capture the hierarchical swapping structure characteristic of this repeater architecture. As previously mentioned, it is a hybrid binary tree structure. But this calculation assumes the total success probability for all swaps occurring simultaneously, which is a calculation based on the Parallel swapping model like Eq. 3.7. In practical scenarios, adopting different swapping orders, such as Sequential or Binary Tree approaches, see Fig 3.8 for details, may yield the same P_{succ} result, yet due to different execution strategies, will lead to different R_{raw} results, as well as variations in control complexity and requirement of memory. This presents a trade-off that must be comprehensively considered. Therefore, the cases are classified and Guha's formula is extended. A further explanation of this result will be provided in Section 3.3.3.

3.3.2 Modelling Extensions to Simulate Realistic Devices (JS)

Guha's [1] architecture requires two types of BSM devices, one within elementary links (EL) to herald entanglement distribution from sources, and another to perform and herald entanglement swapping from quantum memory. Guha's EL analysis [1] is extended to include probabilistic emission of multi-pairs as a function of $P_{\text{em}}(\mu, x)$ in the same manner as in Section 3.2.3. The single link modelling methods are extended to model one photon from each pair interfering at the EL BSM and the other two photons being loaded into or emitted from quantum memory. The success probability of the EL and repeater node is P_e and P_r , respectively, with the former loading and the latter emitting with efficiencies η_{write} and η_{read} . To model EL BSMs with PNR detectors, this results in the updated entanglement distribution probability from one source to one detector in the EL

$$P_{T_{\text{EL}}} = \sum_{x=0}^{\infty} P_{\text{em}}(\mu, x) M_T \eta (1 - \eta)^{(x-1)} \eta_{\text{write}} (1 - \eta_{\text{write}})^{(x-1)} \quad (3.9)$$

$$P_{F_{\text{EL}}} = \sum_{x=0}^{\infty} P_{\text{em}}(\mu, x) (1 - (1 - \eta_{\text{write}})^x) \left[M_F \eta (1 - \eta)^{(x-1)} + (1 - \eta)^x P_{\text{DC}} \right]. \quad (3.10)$$

For non-PNR detectors, the false probability is updated to

$$P_{F_{\text{EL}}} = \sum_{x=0}^{\infty} P_{\text{em}}(\mu, x) (1 - (1 - \eta_{\text{write}})^x) \left[(1 - (1 - \eta)^x) + (1 - \eta)^x P_{\text{DC}} \right]. \quad (3.11)$$

The success probability of the repeater swapping operation from quantum memory P_r is derived by replacing $P_e(\mu, x)\eta_{\text{write}}$ with η_{read} and η with η_d . To ensure the two detectors in the EL BSM detect the correct heralding pattern from the two sources, these probabilities are inputted to Guha's swapping equations [1]. An additional event probability must be added to account for classical correlations producing the correct click pattern at the BSM, based on the probability of at least one detector click. With $P_{\text{ent}} = P_{T_{\text{EL}}} + P_{F_{\text{EL}}}$, Guha [1] defines this probability as $P_{\text{BSM-click}} = 1 - (1 - P_{\text{DC}})(1 - P_{\text{ent}})^2$. The probability of a classical correlation is then $P_{\text{CC}} = P_{\text{DC}}(1 - P_{\text{DC}})[P_{\text{DC}}(1 - P_{\text{BSM-click}}) + P_{\text{BSM-click}}(1 - P_{\text{DC}})]$. Mirroring Section 3.2.3,

$$P_{T-\text{BSM}} = \frac{1}{8} P_{T_{\text{EL}}}^2 (1 - P_{\text{DC}})^2 \quad (3.12)$$

$$P_{F-\text{BSM}} = \frac{1}{8} \left[P_{F_{\text{EL}}}^2 (1 - P_{\text{DC}})^2 + (1 - P_{F_{\text{EL}}})^2 P_{\text{DC}}^2 + 2P_{F_{\text{EL}}} P_{\text{DC}} (1 - P_{F_{\text{EL}}})(1 - P_{\text{DC}}) + P_{\text{CC}} \right]. \quad (3.13)$$

The swapping equations contain a scaling factor of 1/8, which is derived from the fundamental success probability for optical BSMs. When two photons from different entangled pairs interfere on a balanced beam-splitter, a successful Bell-state analysis occurs with a maximum probability of $\frac{1}{2}$ [59]. While Guha does not explain the factor, Zhou [60] motivate its inclusion by explaining how optimal experimental BSMs can distinguish two of the four Bell-states with a probability of 1/2. Since $|\Psi^{\pm}\rangle$ is generated by the source, the BSM can distinguish two different Bell-states with a probability of $\frac{1}{4}$. This is multiplied with the maximum BSM success probability to yield $\frac{1}{8}$, which scales the correct herald probabilities of the BSM detectors

The probability of heralding entanglement swapping with a single frequency is then $P_{\text{BSM-Succ}} = 4(P_{T-\text{BSM}} + P_{F-\text{BSM}})$ with the factor of 4 indicating the four possible states produced from a successful swap operation ($|01, 01\rangle \langle 01, 01|, |01, 10\rangle \langle 01, 10|, |10, 01\rangle \langle 10, 01|, |10, 10\rangle \langle 10, 10|$), resulting in the expected maximum success rate of $\frac{1}{2}$ with perfect transmission. P_e can be improved by increasing frequency mode number M to yield $P_e = 1 - (1 - P_{\text{BSM-Succ}})^M$. The probability of heralding entan-

lement swapping across a repeater chain is then $P_{\text{succ}} = P_e^{N_e} P_{\text{BSM-Succ}}^{(N_e-1)} = P_e^{N_e} P_r^{(N_e-1)}$. The fidelity of the state generated after these swaps can be calculated analytically using Guha's Eq. 24 [1].

3.3.3 Modelling Extensions to Compare Different Swapping Scheme (ZX)

This section focusing on analytical analysing the impact of the following three entanglement swapping schemes on R_{raw} , as illustrated in Fig. 3.8.

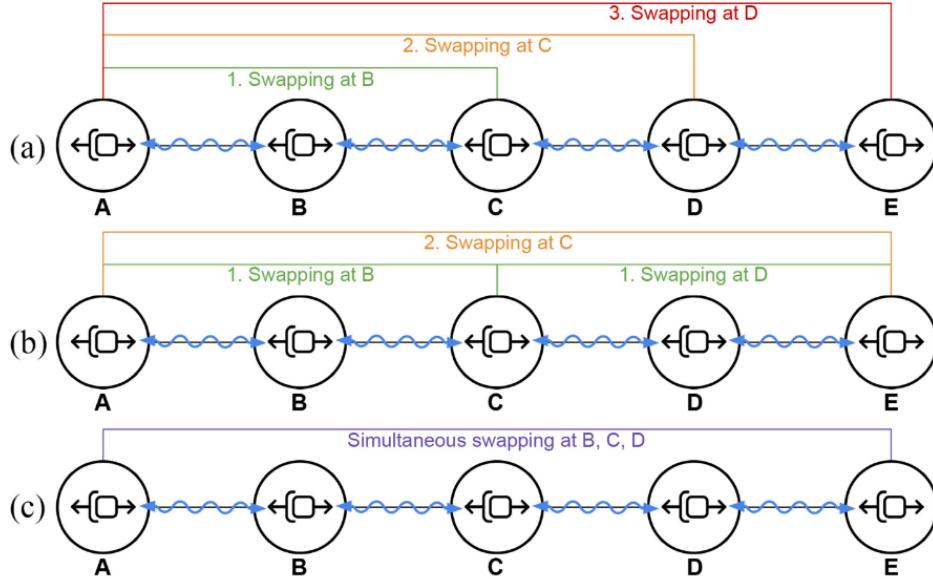


Figure 3.8: Comparison of different entanglement swapping orders (adapted from [26]): (a) Sequential swapping, (b) Binary tree swapping, (c) Parallel swapping.

The three most common entanglement swapping strategies are as follows. In the Sequential swapping method, nodes perform swapping sequentially from left to right. This approach requires $N - 1$ BSMs at each repeater node. Its primary advantage is low control complexity. The Binary Tree structure is one of the most widely studied strategies, and its main benefit is that this scheme takes only $\log_2(N)$ steps. Due to its unique architecture, nodes at the same level can perform swapping in parallel and independently. This strategy is further divided into two variations: the Guha-Binary-tree and the Full-Memory-Binary-tree. The key distinction between these two lies in whether the first-layer repeater nodes in the binary tree structure are equipped with quantum memories. These two strategies will be discussed in more detail later in this section. Finally, the Parallel swapping strategy is not highly scalable because all repeater operations must occur simultaneously. For example, if one swap fails, the whole process must restart. Consequently, the raw key rate drops sharply as the number of repeater nodes increases. However, this strategy can still be advantageous when there are only a few repeater nodes, as it does not require quantum memory, it offers the lowest cost and complexity.

Parameter Setup for derivation of expected generation time

A repeater chain network with $N - 1$ nodes is considered in this analysis. For clarity, the total number of single links is assumed to be $N = 2^n$, which forms a perfect binary tree structure. Each single link attempts to generate an entangled pair (EP) in each round with success probability η_{tr} , and the time duration of one round is denoted as T_q , which is related to the source frequency but limited by the detector dead time. In this analysis, a 1 [MHz] frequency source is employed, resulting in $T_q = 1 \times 10^{-6}$ [s].

Harmonic numbers H_m : The harmonic number H_m quantifies the expected completion time of the last event among multiple independent exponentially distributed events. For example in our work the quantum distribution rate in each single link can be described as $\mathbb{E}[T0] = \frac{T_q}{\eta_{tr}}$ which is a single exponentially distributed event. So in m independent parallel event, Harmonic numbers reflects how the maximum completion time increases compared to the average of a single event. The

expected finished time for m parallel event and the m -th harmonic number H_m is defined as:

$$\mathbb{E}[\max(X_1, \dots, X_m)] = \frac{H_m}{\lambda}, \quad H_m = \sum_{k=1}^m \frac{1}{k}$$

Where $\lambda = \frac{p}{T_q}$ represents the success rate per unit time for each independent event. $\mathbb{E}[T] = \frac{1}{\lambda} = \frac{T_0}{p}$ shows the expected generation time is inversely proportional to the success rate. For example, when $N = 2$ (i.e. one elementary link in Fig 3.7), there are 2 independent parallel events. The expected time of each two link is $\mathbb{E}[T_0] = \frac{T_q}{\eta_{tr}} = \frac{1}{\lambda}$. So the relevant harmonic number and expected generation time becomes:

$$H_2 = 1 + \frac{1}{2} = \frac{3}{2}, \quad \mathbb{E}[\max(X_1, X_2)] = \frac{H_2}{\lambda} \quad (3.14)$$

This directly explains the common coefficient $\frac{3}{2}$ used in expressions like μ_e , where μ_e is the expected time of elementary link operation $\mu_e = \frac{3T_q}{2p_b\eta_{tr}}$, which mentioned from Equation (1) of [10] but they didn't explain why is it. To sum up, it takes into account the fact that, on average, the last among multiple independent operations always takes longer to succeed than single operation which their relationship can be described by Harmonic numbers H_m .

BSM success probability p_b : for the first layer of Guha and Parallel schemes, $p_b = \frac{1}{2}\eta_d$; for the remaining layers of Guha, Full-Memory, and Sequential schemes, $p_b = \frac{1}{2}\eta_d\eta_m^2$, where η_m is the memory efficiency and η_d is the detector efficiency.

Expected BSM delay factor δ , This factor characterizes the probabilistic nature of BSM operations and the latency introduced by herald communication processes which is classical information transmission. $\delta = (t_b + t_c)/p_b$, with t_b denoting detector dead time (20–500 ns) and t_c denoting classical communication delay (assumed to be 20 μ s).

Raw key rate R_{raw} : For all swapping protocols, R_{raw} is defined as the reciprocal of the expected entanglement generation time. The expected time T_{expected} quantifies how long, on average, it takes to successfully generate one end-to-end entangled pair. Since the raw key rate R_{raw} represents the number of raw entangled pairs that can be produced per unit time, it is naturally given by event in a single trial is:

$$R_{\text{raw}} = \frac{1}{T_{\text{expected}}}. \quad (3.15)$$

Derivation of Expected time and Raw key rate for different swapping schemes

Using the swapping scheme principles and parameter setup 3.3.3 introduced above, I derived the expected generation time for different entanglement swapping schemes as shown in Fig 3.8 and presents the corresponding raw key rate equations for simulation. The derivation highlights how architectural differences, such as memory usage or parallelization distribution event influence the expected delay in establishing an end-to-end entangled pair. By combining these expected times, we obtain explicit analytical formulas of R_{raw} that allow a direct performance comparison among the schemes under realistic experimental parameters

Parallel scheme

In the parallel protocol which is the typical **memoryless scheme**, a successful entanglement distribution from Alice to Bob requires all 2^n EPs of elementary links to simultaneously succeed in the same time slot, and all $2^n - 1$ BSM operations to succeed as well. The total success probability of this event in a single trial is:

$$P_{\text{success}}^{\text{parallel}} = \eta_{tr}^{2^n} \cdot p_b^{2^n - 1} \quad (3.16)$$

Hence, the expected time to generate a single end-to-end EP under the waitless protocol is:

$$T_n^{\text{parallel}} = \frac{T_q}{\eta_{tr}^{2^n} \cdot p_b^{2^n - 1}} \quad (3.17)$$

Full memory Binary tree scheme

In the Full memory Binary tree protocol, which is one of the **memory-based scheme**. Each node can store its successfully generated EP in a quantum memory and wait for the sibling link to succeed. After both child links are ready, a BSM is performed. The expected time to generate a single EP over a single link is:

$$T_0^{\text{full}} = \frac{T_q}{\eta_{tr}} \quad (3.18)$$

The expected time to generate a single EP over a elementary link is:

$$T_1 = \frac{3T_q}{2p_b\eta_{tr}} + \frac{t_b+t_c}{p_b} = \mu_e + \delta \quad (3.19)$$

For tree with $N = 2^n$ elementary links. Only the lowest layer requires entanglement generation. Each upper layer only performs BSM operations with stored EPs. The key insight is that at each layer of the binary tree, multiple BSM operations occur in parallel, and the completion time is determined by the slowest of these BSM operations. For the upper layers (levels 2 to $n-1$), the architecture with the Full memory/Guha Binary tree are the same. Each node can store its successfully generated EP in a quantum memory and wait for the BSM to be executed. At each layer k , where $2 \leq k \leq n$, there are $m = \frac{N}{2^k}$ nodes waiting to perform BSM in parallel with the expected delay.

$$T_k^{\text{delay}} = H_m \cdot \delta \quad (3.20)$$

Where $\delta = \frac{t_b+t_c}{p_b}$, $H_m = \sum_{k=1}^m \frac{1}{k}$ is the harmonic number, as mentioned in the Parameter Setup 3.3.3. So for the Full memory binary tree scheme with $N = 2^n$ elementary links, the total expected generation time for one raw key bit is updated to:

$$T_n^{\text{full}} = (\mu + \delta) \cdot H_{N/2} + \sum_{k=2}^n (H_m \cdot \delta) \quad (3.21)$$

Guha Binary tree scheme

In the Guha Binary tree protocol, which is one of the **hybrid memory-based binary tree scheme**. This architecture adopts a memoryless scheme in the first layer enabled by WDM (Wavelength Division Multiplexing) to reduce quantum memory usage, while maintaining memory-based operations in upper layers like Fig.3.7 shows. Each pair of adjacent nodes in the first layer must simultaneously succeed in generating an entangled pair (EP), without memory buffering. Given a per-channel transmission success probability η_{tr} and M WDM channels per link, the effective success probability becomes η_w in Eq. 2.8. So the expected time to generate a single EP over a single link is:

$$T_0^{\text{Guha}} = \frac{T_q}{\eta_w} \quad (3.22)$$

Due to the memoryless nature of the first layer, if the BSM operation fails, the entire process of both single link side must restart from scratch. The expected time to generate a single EP over a elementary link is:

$$T_1 = \frac{T_q}{p_b\eta_w^2} + \delta \quad (3.23)$$

With $N/2$ such nodes operating, so the expected finished time for the first layer is:

$$T_1^{\text{Guha}} = \left(\frac{T_q}{\eta_w^2 \cdot p_b} + \delta \right) \cdot H_{N/2} \quad (3.24)$$

Thus, the total expected entanglement generation time for the n layer Guha binary tree becomes:

$$T_n^{\text{Guha}} = \left(\frac{T_q}{\eta_W^2 \cdot p_b} + \delta \right) \cdot H_{N/2} + \sum_{k=2}^n H_m \cdot \delta \quad (3.25)$$

Sequential scheme

In the sequential protocol, which is the one of the **memory-based scheme** as well, the sequential scheme executes relay operations from left to right. For the first elementary link ($N=2$), the binary tree and sequential schemes are equivalent, so the expected time calculation formula for each is the same, which is

$$T_1^{\text{sequential}} = T_1^{\text{Full}} = \mu \cdot H_2 + \delta \quad (3.26)$$

For links with $N > 2$ segments, since the previous link has already successfully generated half of the qubits and is waiting in storage, only the remaining half of the qubit entangled pairs needs to be generated, So the expected time for that part is

$$T_N^{\text{sequential}} = \frac{T_q}{p_b \cdot \eta_{tr}} + \frac{t_b + t_c}{p_b} \quad (3.27)$$

So the total expected time to generate one end-to-end EP through $N = 2^n$ sequential links is:

$$T_{\text{sequential}}(N) = \frac{1}{p_b} \left[\left(\frac{3}{2} \cdot \frac{T_q}{\eta_{tr}} + t_b + t_c \right) + (N - 2) \cdot \left(\frac{T_q}{\eta_{tr}} + t_b + t_c \right) \right] \quad (3.28)$$

Raw-key-rate equations

Based on the derivation process in Section 3.3.3, which derived the expected generation time T_{expected} (the time required to generate one Raw key bit) under different swapping schemes. Using the relationship $R_{\text{raw}} = \frac{1}{T_{\text{expected}}}$, the raw key rate formulas for these four swapping schemes are:

Sequential scheme:

$$R_{\text{sequential}} = \frac{p_b}{\left(\frac{3}{2} \cdot \frac{T_q}{\eta_{tr}} + t_b + t_c \right) + (N - 2) \cdot \left(\frac{T_q}{\eta_{tr}} + t_b + t_c \right)} \quad (3.29)$$

Guha Binary Tree scheme:

$$R_{\text{Guha}} = \frac{1}{\left(\frac{T_q}{\eta_W^2 \cdot p_b} + \delta \right) \cdot H_{N/2} + \sum_{k=1}^{n-1} H_{m_k} \cdot \delta} \quad (3.30)$$

Full-Memory Binary Tree scheme:

$$R_{\text{full}} = \frac{1}{\mu \cdot H_{N/2} + \sum_{k=0}^{n-1} (H_{m_k} \cdot \delta)} \quad (3.31)$$

Parallel scheme:

$$R_{\text{parallel}} = \frac{\eta_{tr}^{2^n} \cdot p_b^{2^n - 1}}{T_q} \quad (3.32)$$

The equations above shows that the Sequential scheme exhibits linear scaling characteristics, both Binary Tree schemes utilize harmonic numbers to reflect the time amplification effects of parallel operations, while the Parallel scheme's key rate decays exponentially with the number of nodes, making it suitable for short-distance communication scenarios with few repeaters. In Section 4.2, the performance results of different schemes will be presented and analysed. And for these two binary tree scheme, the necessary number of WDM channels M will be discussed to improve the performance of Guha's binary tree structure beyond the full memory binary tree.

3.4 Trusted Node Chain (ZX)

This section shows the workflow of the trusted relay node and the analytical calculation method of the key rate. The core of the trusted relay is to generate the key rate separately in each relay chain, and then decrypt and encrypt (XOR encryption) with the key of the corresponding link at each relay node. The Fig. 3.9 below shows the process of trusted node relay.

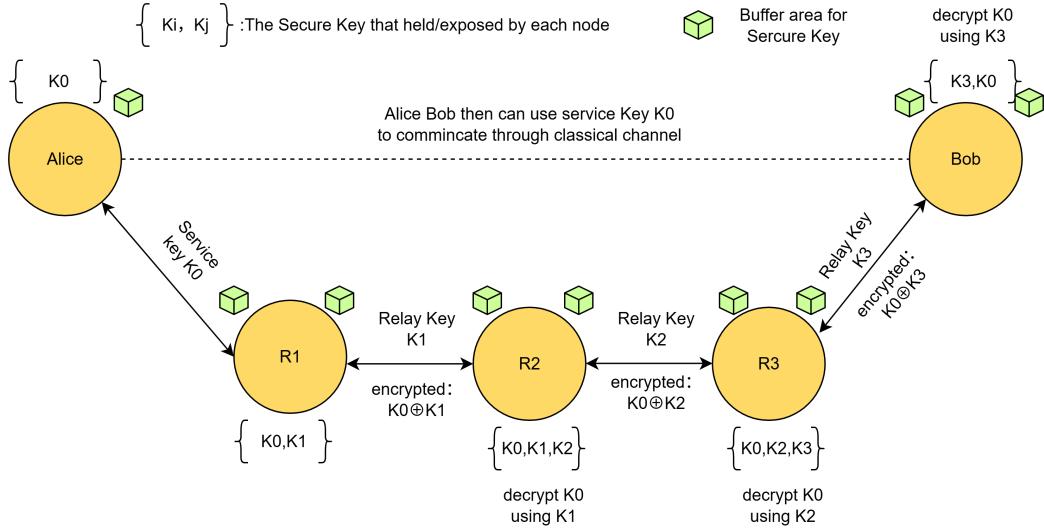


Figure 3.9: Trusted node relay chain workflow. Each node generates keys with adjacent nodes and performs XOR operations to relay the K0.

This section mainly discusses the optimization algorithm for key rate calculation. According to [25], since each node has a buffer area to store the generated service key and wait for the relay key to perform XOR matching, the waiting state and expected waiting time at the relay node will affect the threshold of the key rate, which is not considered by the traditional estimation model [24]. According to Peng's trusted node relay model, which used the Markov chain queuing model to describe this process, the Secure Key Rate(SKR) calculation formula of a single trusted node relay is [25].

$$S_1 = \frac{\eta_{tr0}^2(1 - \mu_1)}{\tau\eta_{tr0}^2(1 - \mu_1) + T_q \left[(1 - \mu_1)(\eta_{tr0} + \mu_1^{M_b}) + \mu_1^{2M_b+1} \right]} \quad (3.33)$$

where $\mu_1 = \frac{\eta_{tr0}(1 - \eta_{tr1})}{\eta_{tr1}(1 - \eta_{tr0})}$, represents the ratio of the Markov chain state transition probability used from Equation(5) of [25], $\tau = \frac{t_q}{L} + \frac{1}{C}$ is the auxiliary variable, Q_p is the size of a raw key packet, M_b the extra buffer size, L is the number of secure key bits in a key packet with $L \leq Q_p$, and C is the classical channel capacity (bps). For a chain with i relay nodes,

$$S_i = \frac{1}{\frac{1}{S_{i-1}} + \gamma_i L} \quad (3.34)$$

where $\gamma_i \propto \frac{1}{\eta_{tr_i}}$. In Section 4.3, the calculation results of Peng's queuing model (Eq. 3.34) and traditional methods (Eq.2.6) will be compared based on the simulation results to illustrate the rationality of the Peng's results. At the same time, the optimal number of relays for any given distance will be discussed based on the formula

$$|R|_{\text{opt}} = \arg \max_{1 \leq r \leq D} S_r \left(\frac{D}{r+1+\Delta} \right) \quad (3.35)$$

where D is the total distance between Alice and Bob, and $\Delta > 0$ is the distance allocation parameter. Let $r \in \mathbb{Z}^+$ be a positive integer which means the number of relays.

3.5 QM Mathematical Model for EIT and Off-Resonant Raman (CM)

The mathematical formalism in [30] describes an atomic ensemble in a cavity for quantum memory applications. In this model, the atomic polarisation P and spin-wave S evolve according to Eq. 3.36,

$$\begin{aligned}\dot{P} &= -[\gamma(1+C) + i\Delta]P + i\Omega S + i\sqrt{2\gamma C}E_{\text{in}}, \\ \dot{S} &= i\Omega^* P,\end{aligned}\quad (3.36)$$

where γ is the polarisation decay rate, E_{in} is the temporal input field, and C is the cooperativity (effective optical depth in the cavity).

In the adiabatic limit ($\dot{P} = 0$), the optimal storage control field is presented in Eq. 3.37 below,

$$\Omega(t) \propto -\frac{\gamma(1+C) - i\Delta}{\sqrt{2\gamma(1+C)}} \frac{E_{\text{in}}(t)}{\sqrt{\int_0^t |E_{\text{in}}(t')|^2 dt'}}, \quad (3.37)$$

with phase irrelevant for efficiency. The adiabatic condition is $TC\gamma \gg 1$, where T is the input pulse duration. Under this condition, both the near-resonant EIT regime ($\gamma C \gg |\Delta|$) and the off-resonant Raman regime ($\gamma C \ll |\Delta|$) reach the maximum retrieval efficiency $\eta_{\text{read}} = \frac{C}{1+C}$, provided the control field is long enough to prevent residual excitation. In the Raman limit, satisfying the adiabatic condition requires stronger Ω , increasing susceptibility to FWM noise.

For a Gaussian-like input, the optimal storage control from Eq. 3.37 can be used to solve Eq. 3.36 without the adiabatic approximation to obtain $S(t)$. The total efficiency is calculated as $\eta_{\text{qm,tot}} = \eta_{\text{read}}\eta_{\text{write}} = \eta_{\text{read}}|S|^2$. Thus, maximum efficiency, with a non-zero spin-wave decay rate γ_s , can be calculated using Eq. 3.38 below,

$$\eta_{\text{qm,max}} = \left(\frac{C}{1+C}\right)^2 e^{-2\gamma_s \tau_s}. \quad (3.38)$$

Fidelity is given by $F = (1 + \eta_{\text{qm,tot}})/2$, hence minimum retrieval fidelity is 50%.

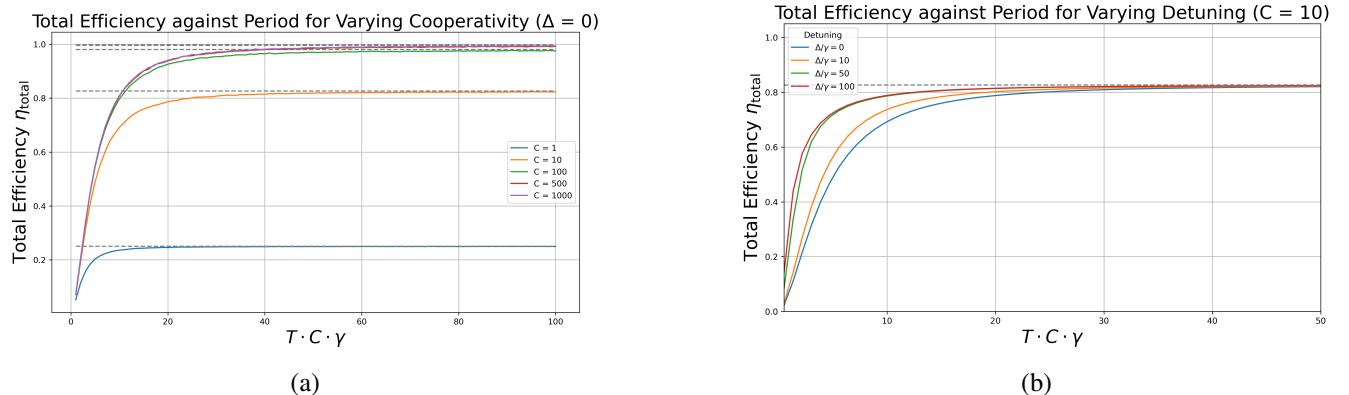


Figure 3.10: (a) Total efficiency in the EIT regime ($\Delta = 0$), for $\gamma = 1$ and $\gamma_s = 0$, plotted as a function of $TC\gamma$ (adiabatic parameter). Curves correspond to $C = 1, 10, 100, 500, 1000$, with horizontal dashed lines showing the maximum efficiency $\eta_{\text{qm,max}} = (C/(1+C))^2$. (b) Same plot for off-resonant Raman limit using $C = 10$ and $\Delta/\gamma = 0, 1, 10, 50, 100$. In both regimes, efficiencies tends to η_{max} when $TC\gamma \gg 1$. These plots are reproductions of Fig. 2 from [30].

The characterisation of the cavity-based model for EIT and Raman protocols is shown in Fig. 3.10. Both can, in principle, achieve the same maximum efficiency under the adiabatic condition. However, the Raman protocol supports shorter input pulses before breakdown, indicating higher bandwidth. Fig. 3.10a shows that efficiency saturates beyond a certain optical depth, while Fig. 3.10b shows that increasing detuning only marginally reduces the pulse duration limit. This model, however, offers only a partial description of hot-vapour memories, which are more accurately captured by free-space models [61]. Nonetheless, since the free-space approach builds on the cavity formalism, the cavity model still offers useful insight into the operation of these protocols and justifies the use of the approximation $\eta_{\text{read}} \approx \eta_{\text{write}}$.

Interestingly, Fig. 3.10 shows a trend similar to the AFC efficiency in Fig. 3.11a, taken from [33]. In AFC, saturation is set by finesse rather than optical depth. Finesse describes the sharpness of the comb peaks, linked to material properties. This parallel highlights a common principle, where both cavity-based and AFC models have limiting parameters that cap efficiency, underscoring the universal need to optimise absorption–emission trade-offs in quantum memories.

Fig. 3.11b shows that retrieval fidelity decreases with increasing spin-wave decay, reflecting the exponential efficiency loss for non-zero decay. Such exponential decay from spontaneous emission is a feature common to all protocols.

Overall, the results highlight the importance of balancing parameters, e.g. control-field, to maximise efficiency while suppressing noise, and they underscore the role of decay rates in preserving the integrity of stored states. Further refinements are therefore needed for more realistic modelling. Nevertheless, the insights gained here are broadly applicable when assessing which type of quantum memory best suits a given repeater architecture.

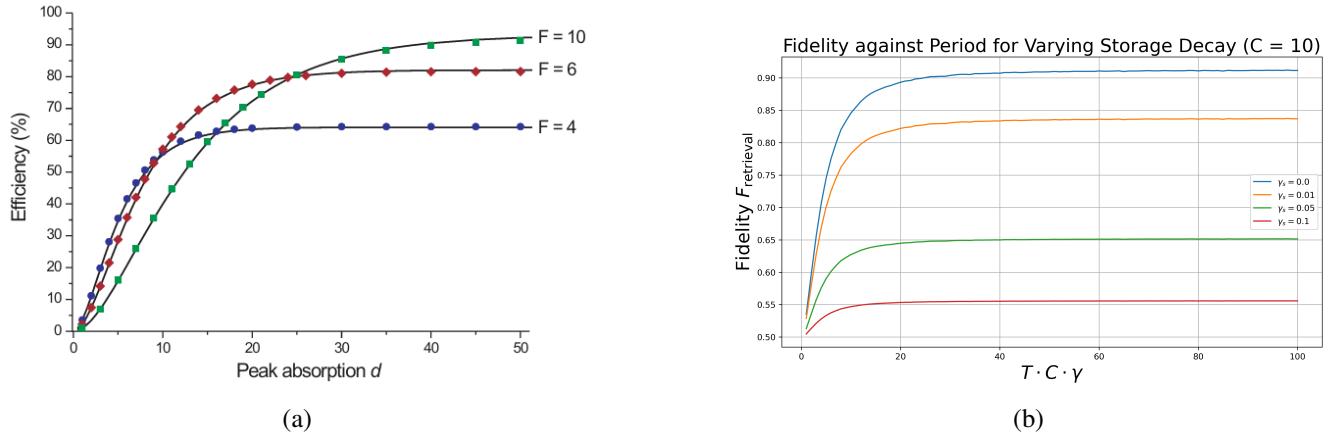


Figure 3.11: (a) AFC efficiency versus peak absorption for finesse values $F = 4, 6, 10$. Higher finesse yields sharper comb teeth and higher saturation efficiency. Taken from Fig. 2 of [33]. (b) Retrieval fidelity in the EIT regime ($\Delta = 0, C = 10$) versus adiabatic parameters. Increasing γ reduces the maximum fidelity.

3.6 Quantum Error Correction (JMa)

In QKD systems, the dominant noise sources are (i) photon loss in the optical channel and (ii) decoherence in the quantum memory. Two complementary quantum error correction (QEC) schemes are implemented to be tailored to these domains: a Generalized Quantum Parity Code (GQPC) to mitigate transmission loss, and the five-qubit [[5,1,3]] stabilizer code to correct memory errors. Notably, the QKD platform employs time-bin entanglement, which is intrinsically robust against fibre phase noise and polarization drifts. For example, time-bin entangled photon pairs exhibit strong immunity to fibre decoherence and polarization scattering [62]. This leaves photon loss as the primary channel impairment, for which code-based one-way repeaters (e.g. quantum Reed–Solomon codes [40]) and parity-encoding schemes [63] are well-suited. Meanwhile, for quantum memory, the five-qubit code is known to be one of the optimal small-size QEC codes for preserving qubit coherence [64]. In the following, the design and impact of each QEC approach are discussed with respect to repeater system performance.

3.6.1 QEC for Loss in One-Way Quantum Channels: Generalized QPC

For long-distance transmission through lossy fiber, the most severe error is photon loss (an erasure error). Quantum parity codes (QPC) and related loss-tolerant encodings have been widely adopted in one-way quantum repeater schemes based on linear optics and BSMs [40], [45]. The redundant QPC introduced by Munro [45] concatenates two levels of repetition coding to protect against photon loss without requiring quantum memories. However, a limitation of the original QPC is that its success probability exhibits large discrete jumps as the code length N increases, because N must be factorizable into fixed-size inner blocks ($N = n \times m$) leading to suboptimal use of available qubits.

The recently proposed Generalized Quantum Parity Code (GQPC(m_1, m_2, \dots, m_n)) [65] is employed, which generalizes the QPC by allowing a flexible set of inner block lengths $\{m_i\}$ instead of a fixed m . In a GQPC encoding, $N = \sum_{i=1}^n m_i$ physical qubits (photons) carry one logical qubit, using a concatenated parity-check structure where each block of m_i photons is parity-

protected and the blocks are further parity-encoded together. By optimizing the length distribution $\{m_i\}$ without increasing hardware complexity, GQPC leverages all available qubits to boost loss tolerance continuously, avoiding the performance “cliff” of the original parity code. In essence, GQPC provides a more stable and higher success rate for logical BSMs under loss, given the same total number of photons, compared to the standard QPC encoding. This makes GQPC especially suitable for ultrafast one-way repeaters based on linear optics [65].

Performance and Rate: The logical BSM success probability of a GQPC code with inner block lengths $\{m_i\}$ and per-photon transmission η is given by [65]:

$$P = \prod_{i=1}^n [1 - (1 - \eta)^{m_i}] - \prod_{i=1}^n \left[1 - (1 - \eta)^{m_i} - \frac{\eta^{m_i}}{2} \right]. \quad (3.39)$$

This expression reflects the probability that, across all inner code blocks, at least one photon survives transmission and can contribute to a successful logical BSM outcome, corrected by subtracting cases where the surviving photons do not yield a valid Bell-state signature. The success probability P thus encapsulates the enhanced loss tolerance provided by GQPC relative to conventional parity codes.

Given M repeater segments, the end-to-end success probability is

$$P_{\text{tot}} = P^M. \quad (3.40)$$

Equivalently, $P_{\text{tot}} = P^{L_{\text{tot}}/L_0}$ [65], where L_0 is the elementary segment length and L_{tot} the total distance. The end-to-end transmission success rate characterizing the overall quantum communication scheme can be written as $R = P_{\text{tot}}/t_0$, where t_0 denotes the minimal processing time per station (optimistically ~ 1 ns for static linear optics [63]).

In addition, Ewert [63] propose the resource cost function that, in their framework, has a direct physical meaning as the average photon expenditure per successful logical transmission (i.e. the average photon overhead):

$$\text{Cost}_{\text{photons}} = \frac{N}{R t_0 L_0}, \quad (3.41)$$

where N is the total number of physical photons in the code block, R is the logical transmission success rate, and L_0 is the elementary segment length. This metric provides a resource-normalized benchmark for comparing GQPC with other loss-tolerant strategies. This is denoted $\text{Cost}_{\text{photons}}$ (rather than C) to avoid confusion with the cooperativity C that appears in the memory-interface model. Under this metric, GQPC maintains favorable efficiency while scaling smoothly with the available photon number N .

Limitations: The above performance analysis assumes an idealized noise model limited to photon loss. Detector inefficiencies, dark counts, mode mismatches, and operational errors are neglected. In practice, these additional errors will need to be addressed via more comprehensive QEC or fault-tolerance techniques. Nonetheless, within the loss-dominated scenario for which GQPC was designed, our QKD repeater chain gains significantly in success probability and rate without requiring quantum memories (a hallmark advantage of the one-way repeater paradigm [45]).

3.6.2 QEC for Quantum Memory Noise: Five-Qubit Code

Each repeater node in the system contains a Λ -type atomic quantum memory that stores a single-photon qubit (time-bin encoded) as an atomic excitation. This allows entangled photons to be temporarily held at intermediate nodes to enable BSMs for entanglement swapping. However, while waiting for classical heralding signals across the chain, the quantum memory qubits are subject to decoherence and noise. To preserve the entanglement fidelity during these wait times, the [[5,1,3]] five-qubit quantum error-correcting code (the “perfect” code) [64], [66], [67] is employed. This code encodes one logical qubit into five physical qubits and can correct any single-qubit error (arbitrary Pauli X , Y , or Z) on any one of the five physical qubits. With distance $d = 3$, it is the minimum-size code capable of correcting one error on a general unknown state.

Periodic Memory Correction: The five-qubit stabilizer code is integrated into a periodic correction cycle. A stored photonic qubit is first encoded across five physical qubits in the memory node. During each waiting period τ , any single error can be detected by measuring the stabilizers and corrected via the appropriate Pauli recovery. The cycle repeats throughout the total storage duration T , resulting in $N = T/\tau$ (with a final remainder Δ if $T \neq N\tau$). This active cycling prevents error

accumulation and thus extends the effective coherence time of the memory.

As a baseline intuition, if the memory's spin decoherence is characterized by a per-qubit rate γ , then without QEC the single-qubit error probability over duration T is $p(T) = 1 - e^{-2\gamma T}$ (survival probability $1 - p(T)$).

With QEC, errors are modelled on any interval $x \in [\tau, \Delta]$ by independent and identically distributed error-rate function

$$p(x) = 1 - e^{-2\gamma x}. \quad (3.42)$$

Because the $[[5, 1, 3]]$ code corrects any single physical error in a five-qubit block, independence gives the block success probability

$$P(x) = (1 - p(x))^5 + 5p(x)(1 - p(x))^4 = e^{-8\gamma x}(5 - 4e^{-2\gamma x}). \quad (3.43)$$

Writing $T = N\tau + \Delta$ with $N = \lfloor T/\tau \rfloor$ and $0 \leq \Delta < \tau$, cycles multiply after each syndrome reset, hence the logical survival probability is

$$P_{\text{logic}}(T) = [P(\tau)]^N P(\Delta). \quad (3.44)$$

Including the store/retrieve interface (see section 3.5 of the main paper; $\eta_{\text{retr}} = C/(1+C)$ each way), the overall memory efficiency and the serial qubit cost (one ancilla, $n_q = 5 + 1 = 6$) are

$$\eta_{\text{QEC}}(T) = \left(\frac{C}{1+C} \right)^2 P_{\text{logic}}(T), \quad \text{Cost}_{\text{qubits}}(T) = \frac{6}{\eta_{\text{QEC}}(T)}. \quad (3.45)$$

In practice, implementing the five-qubit code in Λ -type atomic memory requires either entangling operations between a small register of atomic qubits or mapping the photonic qubit into such a register. Each QEC cycle performs syndrome measurements and a Pauli recovery and must complete within the correction window τ . Under the i.i.d. error model, as long as at most one physical error occurs per interval τ , the cycle corrects it and prevents accumulation across the N cycles in $T = N\tau + \Delta$. The probability that an uncorrectable event (two or more errors in one cycle) occurs scales as $O((\gamma\tau)^2)$, hence choosing $\tau \ll 1/\gamma$ strongly suppresses logical failures. In the small-error regime $p(x) \ll 1$, the block success admits the expansion $P(x) = 1 - 10p(x)^2 + O(p(x)^3)$, making explicit that first-order physical errors are removed at the logical level.

Limitations: The analysis focuses on a loss/decoherence-dominated memory model and neglects errors introduced by the QEC operations themselves (gate infidelity, measurement errors, leakage, crosstalk). If such overhead is non-negligible, one should replace τ by an effective $\tau_{\text{eff}} = \tau - t_{\text{QEC}}$ in the above expressions and include additional failure channels in $P(x)$. We also assume independent per-qubit errors and a Pauli-type channel, and we treat the store/retrieve factor $\eta_{\text{retr}} = C/(1+C)$ as constant; relaxing these assumptions would slightly reduce $P_{\text{logic}}(T)$ and $\eta_{\text{QEC}}(T)$ and is left for future system-level refinements.

3.7 Entanglement Purification Module (JMa)

We developed an entanglement purification (EP) module for the QKD system simulator, incorporating three different entanglement distillation protocols and several functional components. The protocols implemented are: (1) a nested DEJMPS protocol, (2) a multi-copy nested entanglement purification protocol, and (3) a frequency–polarization hyperentanglement protocol. In addition, the module includes three key functional features: measurement-based purification, Reset-and-Reuse, and theoretical limit evaluation.

3.7.1 Functional Modules

Measurement-Based Purification. Most entanglement purification protocols typically neglect the effect of measurement noise. However, as shown in [68], although measurement noise has little impact on the final fidelity and success probability, it can significantly raise the effective fidelity threshold L required for successful purification (the minimum input state fidelity for which purification is effective). Therefore, our module models and compensates for measurement noise in order to lower this effective threshold and ensure the purification operation remains viable. This requires balancing the improvement in measurement accuracy against the reduction in overall yield. Following the standard depolarizing noise model from [68],

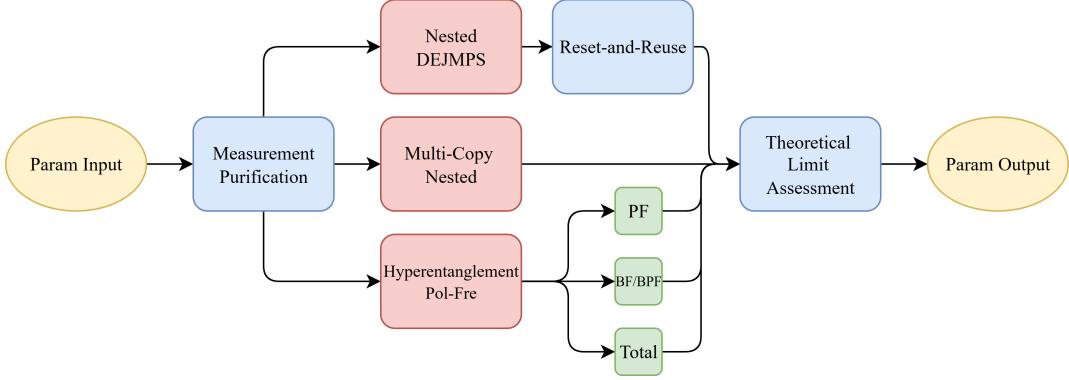


Figure 3.12: Entanglement purification module structure flowchart.

we represent the noisy measurement operators and resulting fidelity as:

$$\tilde{M}_i = \left(1 - \frac{p_m}{2}\right) M_i + \frac{p_m}{2} M_{i\oplus 1}, \quad F_{\text{noisy}} = \left(1 - \frac{p_m}{2}\right) F + \frac{p_m}{2} (1 - F). \quad (3.46)$$

Here p_m is the measurement error probability. Limitations: Ref. [68] indicates that measurement-based purification is not well-suited to protocols involving many CNOT gates (the robustness degrades with numerous CNOT operations). The multi-copy nested protocol is one such multi-CNOT protocol. Moreover, the input fidelity thresholds of the multi-copy nested protocol and the frequency–polarization hyperentanglement protocol are essentially unaffected by measurement noise. Thus, for those two protocols, the measurement-purification feature is used primarily to examine how noise impacts their fidelity and success probability, rather than to lower a threshold.

Theoretical Limit Evaluation. This module evaluates each protocol’s performance against fundamental entanglement distillation limits. We include the asymptotic hashing bound for Werner states as a point of reference [46], [66], [69], [70]. Under the restriction of one-way classical communication (the hashing protocol scenario), the maximum number of perfect Bell pairs distillable per Werner state (the asymptotic rate) is given by:

$$E_{\text{hash}}(F) = 1 - S(\rho_W) = 1 + F \log_2 F + (1 - F) \log_2 \left(\frac{1 - F}{3} \right). \quad (3.47)$$

Meaning: For a large number of Werner states all with fidelity F , in theory at most $E_{\text{hash}}(F)$ perfect Bell pairs can be asymptotically extracted per input pair. Threshold: The hashing protocol yields a positive rate only if $E_{\text{hash}}(F) > 0$ (i.e. $F \gtrsim 0.8107$); below this fidelity (approximately 0.81), the protocol has zero net yield.

We also define an overall performance metric R to compare purification protocols. R quantifies the number of noiseless Bell pairs (ebits) obtained per input pair when one round of a given purification protocol is followed by an optimal one-way hashing distillation. In formula form,

$$R = P_{\text{succ}} \frac{E_{\text{hash}}(F_{\text{out}})}{n_{\text{in}}} = \frac{E_{\text{hash}}(F_{\text{out}})}{N_{\text{avg}}/2}. \quad (3.48)$$

Here F_{out} is the output fidelity after one purification round, P_{succ} is the protocol’s success probability, n_{in} is the number of input entangled pairs consumed in the round, and $N_{\text{avg}}/2$ represents the average number of input pairs consumed per output pair (accounting for the possibility of failure). Thus, R reflects the average yield (ebits per input pair) of a “purify + hash” composite strategy, taking into account (1) the fidelity improvement achieved (F_{out}), (2) the success probability P_{succ} , and (3) the resource consumption n_{EP} (number of input pairs used) in the purification round. Unlike comparing just output fidelity or success probability alone, this metric R provides a more holistic measure of protocol performance under finite resources, making it especially useful for cross-comparing different entanglement purification schemes. Note: R does not directly correspond to the hashing bound of the input state $E_{\text{hash}}(F_{\text{in}})$, but rather to the overall efficiency after one round of purification plus ideal hashing. Consequently, in certain regimes R can exceed the direct hashing bound of the initial state; however, it will always

remain limited by the ultimate theoretical bound on distillable entanglement.

Reset-and-Reuse. To extend entanglement to long distances, quantum repeaters must perform entanglement distillation, but current quantum hardware is severely resource-constrained (few qubits with high noise). Multi-round entanglement distillation (multi-pass protocols) would ordinarily require an exponentially growing number of fresh qubits for each round and has lacked real-time feed-forward, making it infeasible experimentally. The reset-and-reuse technique [71] addresses this by utilizing mid-circuit qubit resets (available on IBM Q devices since 2021). After measuring auxiliary qubits, those qubits are reset to $|0\rangle$ and immediately reused in subsequent rounds. This allows multi-round distillation to consume a fixed number of physical qubits independent of the number of rounds (rather than requiring new qubits each round). In [71], this approach was demonstrated for the BBPSSW and DEJMPS protocols, with substantial resource savings. We apply the same idea to our nested DEJMPS protocol, which dramatically reduces qubit resource requirements (e.g. multiple purification rounds can be run using the qubits from a single round). Limitations: Ref. [71] also found that the DEJMPS protocol's performance gains saturate or even degrade after the second round (fidelity drops significantly after too many rounds, although the entanglement distribution success probability does improve). Overall, the multi-pass protocol showed only modest performance improvement, insufficient to fully overcome noise. In our module, we therefore neglect the potential effects of mid-circuit resets on fidelity and success probability, and consider this technique only in terms of resource consumption. This allows us to evaluate how reset-and-reuse could impact the overall performance of multi-round protocols in a future quantum repeater scenario, focusing on resource-success-fidelity trade-offs.

3.7.2 Entanglement Purification Protocols

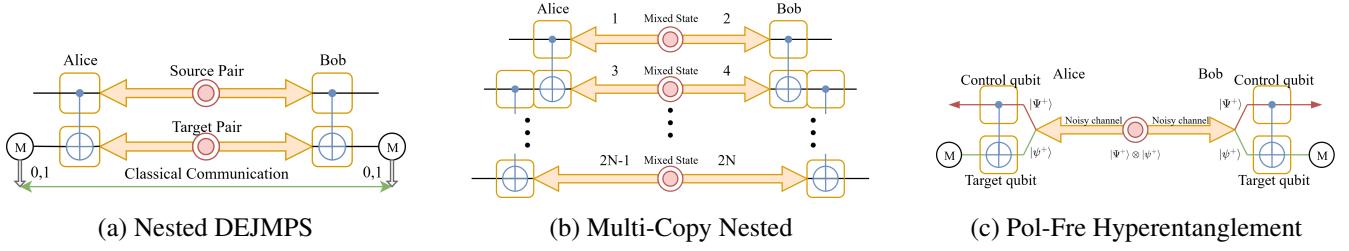


Figure 3.13: Schematic illustration of an entanglement purification scheme

Nested DEJMPS Protocol. The DEJMPS protocol [47] is a well-known two-pair entanglement purification method. We implement a nested version of DEJMPS (up to k rounds) by applying the original DEJMPS operations recursively (with appropriate twirling of states between rounds). From the standard theory, we obtain analytic expressions for the fidelity and success probability after k nesting levels. Ignoring measurement noise for the moment, the output fidelity after k rounds (with k the nesting depth) is:

$$F^{(k)} = \frac{(F^{(k-1)})^2 + \frac{1}{9}(1 - F^{(k-1)})^2}{(F^{(k-1)})^2 + \frac{2}{3}F^{(k-1)}(1 - F^{(k-1)}) + \frac{5}{9}(1 - F^{(k-1)})^2}, \quad F^{(0)} = F_{\text{in}}. \quad (3.49)$$

The success probability of one round (taking two input pairs to one output pair) as a function of fidelity F is

$$p_{\text{succ}}(F) := F^2 + \frac{2}{3}F(1 - F) + \frac{5}{9}(1 - F)^2, \quad (3.50)$$

and the overall success probability after n_{DEJMPS} rounds (without mid-circuit resets) is the product of each round's success probability:

$$P_{\text{SUCC}}^{(n_{\text{DEJMPS}})} = \prod_{k=1}^{n_{\text{DEJMPS}}} p_{\text{succ}}(F^{(k-1)}). \quad (3.51)$$

The resource consumption for k nested rounds (without reset) is $2 \times (k + 1)$ entangled pairs (since each round uses two pairs, with one pair output to the next round). If the Reset-and-Reuse feature is employed, the resource cost reduces to a constant 4

qubits (effectively the resources of a single round are reused for all rounds).

When measurement noise is included, we restrict to a single nesting round ($k = 1$) and apply measurement-based purification. In this case, according to [68] the output fidelity is:

$$F_{\text{out}} = \frac{F^2 + \left(\frac{1-F}{3}\right)^2 + g^{(n,m)}(F)}{F^2 + 2F\left(\frac{1-F}{3}\right) + 5\left(\frac{1-F}{3}\right)^2 + 4g^{(n,m)}(F)}. \quad (3.52)$$

The term $g^{(n,m)}(F)$ accounts for cases where an odd number of measurement outcomes indicate bit-flip errors:

$$g^{(n,m)}(F) = \left(\frac{F(1-F)}{3} + \left(\frac{1-F}{3}\right)^2 \right)^{\frac{r_{\text{odd}}^{(n,m)}}{r_{\text{even}}^{(n,m)}}}, \quad (3.53a)$$

$$r_{\text{even}}^{(n,m)} = \left(1 - \frac{p_m}{2}\right)^n \left(1 - \frac{p_m}{2}\right)^m + \left(\frac{p_m}{2}\right)^n \left(\frac{p_m}{2}\right)^m, \quad (3.53b)$$

$$r_{\text{odd}}^{(n,m)} = \left(1 - \frac{p_m}{2}\right)^n \left(\frac{p_m}{2}\right)^m + \left(\frac{p_m}{2}\right)^n \left(1 - \frac{p_m}{2}\right)^m. \quad (3.53c)$$

Here n and m are the numbers of qubits (or measurements) used by the two parties (A and B) during the measurement-based purification. For simplicity (to reduce simulation complexity), we assume identical measurement noise on both sides and in each operation. Note that when $n = m = 1$, no measurement-based purification is effectively applied (this case corresponds to simply having measurement noise without any noise-mitigation procedure). In that limit $g^{(1,1)}(F) = 0$ and F_{out} reduces to the standard DEJMPS formula. We can also derive the effective fidelity threshold L for which a noisy measurement purification still yields a fidelity improvement:

$$L^{(n,m)} = \frac{r_{\text{even}}^{(n,m)} + r_{\text{odd}}^{(n,m)}}{2(r_{\text{even}}^{(n,m)} - r_{\text{odd}}^{(n,m)})}. \quad (3.54)$$

This $L^{(n,m)}$ is the minimum input fidelity for which the entanglement purification succeeds in raising the fidelity in the presence of measurement noise.

Limitations & challenges: As the number of nesting rounds increases, the resource requirement grows rapidly. The presence of measurement noise significantly affects the effective fidelity threshold L , making high-fidelity inputs necessary. Moreover, in this study we have not incorporated the effect of photon transmission loss on the success probability, which remains an important factor for real-world implementations.

Multi-Copy Nested Protocol [72]. This protocol distills one high-fidelity entangled pair from N low-fidelity pairs in a single collective operation, extending the entanglement distribution distance and supporting quantum repeaters. Photons are passed through cascaded polarizing beam splitters (PBSs) to filter out noise based on their output spatial modes: Photons are passed through cascaded polarizing beam splitters (PBSs) to filter out noise based on their output spatial modes: in the ideal Bell-state case, the two photons from a given pair exit into different output modes; double-pair noise causes both photons from some pairs to exit into the same output mode (these events are discarded by the PBS filters); and we post-select events in which $2n$ output modes each contain exactly one photon (e.g., a four-mode or six-mode coincident-detection scheme). For such events, the output fidelity F_{out} and success probability P_{succ} can be expressed as:

$$F_{\text{out}} = \frac{a}{a+b}, \quad P_{\text{succ}} = a+b. \quad (3.55)$$

where a and b are the normalized probabilities of obtaining, respectively, a desired Bell state or an undesired state in the post-selected event. In general,

$$a_x = \alpha_x F^N + \beta_x (1-F)^N, \quad (3.56a)$$

$$b_x = \alpha_x (1-F)^N + \beta_x F^N. \quad (3.56b)$$

The coefficients (α_x, β_x) depend on the noise scenario:

$$(\alpha_x, \beta_x) = \begin{cases} (1, 0), & \text{noiseless case,} \\ \left(1 - \frac{p_m}{2}, \frac{p_m}{2}\right), & \text{with measurement noise } p_m, \\ (r_{\text{even}}, r_{\text{odd}}), & \text{with measurement purification.} \end{cases}$$

where r_{even} and r_{odd} are the probabilities of an even or odd number of measurement-bit flips (respectively) when n measurements are used:

$$r_{\text{even}}(n) = \sum_{\substack{j=0 \\ j \text{ even}}}^n \binom{n}{j} \left(\frac{p_m}{2}\right)^j \left(1 - \frac{p_m}{2}\right)^{n-j} = \frac{1 + (1 - p_m)^n}{2}, \quad (3.57\text{a})$$

$$r_{\text{odd}}(n) = \sum_{\substack{j=0 \\ j \text{ odd}}}^n \binom{n}{j} \left(\frac{p_m}{2}\right)^j \left(1 - \frac{p_m}{2}\right)^{n-j} = \frac{1 - (1 - p_m)^n}{2}. \quad (3.57\text{b})$$

In this multi-copy protocol, the required input fidelity threshold remains the same as the standard case ($> 1/2$ for distillable entanglement).

Limitations & challenges: Resource consumption increases with N , requiring a larger number of entangled pairs and detectors; for example, a six-mode scheme needs 12 single-photon detectors. In addition, we have not accounted for photon transmission losses, which in practice will reduce the success probability of this protocol.

Polarization–Frequency Hyperentanglement Protocol [73]. This protocol uses photons that are hyperentangled—each photon pair is simultaneously entangled in polarization and frequency degrees of freedom (DOFs). Specifically, the source produces photon pairs in a state entangled in polarization (e.g. $|\Psi^+\rangle$ Bell state) and in frequency (e.g. $|\psi^\pm\rangle$). An equivalent CNOT operation is implemented with polarization as the control bit and frequency as the target bit, using a polarization-dependent frequency converter. Through postselection, events where the photons' frequency state collapses to $|\phi^\pm\rangle$ are kept, while events resulting in $|\psi^\pm\rangle$ are discarded. This postselection removes errors corresponding to polarization bit-flips (BF) and bit-phase-flips (BPF) on the polarization-encoded qubit. The scheme offers inherent noise resilience: in a linear optical channel, the frequency-encoded qubit is immune to bit-flip errors (BF or BPF errors arise only via nonlinear effects). It is also highly efficient: entanglement purification operates on a single photon pair (no need for multiple pairs), yielding rates 5–7 orders of magnitude higher than traditional two-pair schemes (e.g. compared to conventional PET/PSM protocols). Moreover, it is compatible with existing fiber-optic networks, since the frequency degree of freedom is well-suited for long-distance transmission.

We analyze three error scenarios for the hyperentangled state (with F_p denoting the initial polarization Bell-state fidelity):

Scenario 1: Only BF/BPF errors occur (phase-flip errors $A = 0$).

Scenario 2: Only phase-flip (PF) errors occur ($B = C = 0$, no bit-flip errors).

Scenario 3: Mixed errors (both PF and BF/BPF errors present).

Let A , B , and C be the probabilities of a phase-flip error, a bit-flip error, and a joint bit-phase-flip error, respectively, so that $F_p + A + B + C = 1$. The frequency conversion efficiency is denoted by η (with current experimental values up to $\sim 57\%$ [74]). Non-unit frequency conversion efficiency $\eta < 1$ degrades the purification outcome—indeed, even if the intrinsic fidelity in the frequency domain F_f is high, a low η will reduce the final polarization fidelity F'_p after purification. Depending on the error scenario, the output fidelity and success probability are given by:

$$\text{Scenario 1: } F_{\text{out}} = \frac{aF_p}{F_p + (1 - \eta)(1 - F_p)}, \quad P_{\text{succ}} = F_p + (1 - \eta)(1 - F_p), \quad (3.58\text{a})$$

$$\text{Scenario 2: } F_{\text{out}} = aF_p + b(1 - F_p), \quad P_{\text{succ}} = 1, \quad (3.58\text{b})$$

$$\text{Scenario 3: } F_{\text{out}} = \frac{aF_p + bA}{F_p + A + (1 - \eta)(B + C)}, \quad P_{\text{succ}} = F_p + A + (1 - \eta)(B + C). \quad (3.58\text{c})$$

Here a and b are functions of the initial joint state parameters, analogous to those in Eqs. (3.56a)–(3.56b). The resource consumption for this hyperentanglement protocol (if augmented with n -pair measurement purification) is $2(n+1)$ photons (two photons for the main hyperentangled pair, plus $2n$ for ancillary pairs if n rounds of measurement-based purification are used). We can again express a_x and b_x in the generic form:

$$a_x = \alpha_x F_f + \beta_x (1 - F_f), \quad (3.59a)$$

$$b_x = \alpha_x (1 - F_f) + \beta_x F_f, \quad (3.59b)$$

with (α_x, β_x) taking the values (noiseless), (with noise p_m), or $(r_{\text{even}}, r_{\text{odd}})$ (with measurement purification) as defined earlier.

Limitations & challenges: The currently achievable frequency-conversion efficiency (around 50%) constrains the entanglement yield; approaching ideal performance will require improved designs of nonlinear waveguides or converters. In regimes dominated by phase errors (Scenario 2), an additional corrective step (e.g., a Hadamard on the polarization qubit) is needed to interchange the $|0\rangle/|1\rangle$ basis and thereby convert phase errors into detectable bit-flip errors. Moreover, polarization entanglement can drift over long-distance fiber links, necessitating active polarization tracking and compensation [75], [76].

3.8 Integration of Models in the Simulator (JS, JMc, JMa)

Distributing a Single Entangled Pair: The methods described in this section can be interfaced to yield a full simulation of a repeater chain network. First, the link hardware model (e.g. Guha or realistic hardware) is chosen with the corresponding hardware parameters. The initial P_{ent} and F_{ent} of entanglement distribution before noisy quantum memory is first calculated (Section 3.3.2). Then, a swapping scheme is selected which provides the corresponding expected time qubits spend idling in memory waiting for all swapping operations to succeed, T_{expected} . P_{ent} is inputted to the scheme’s corresponding R_{raw} calculation, such as Eq. 3.8 for the Parallel swapping scheme. This yields $T_{\text{expected}} = \frac{1}{R_{\text{raw}}}$ as shown in Eq. 3.15. This idle time and initial F_{ent} are inputted as parameters to the chosen quantum memory, which has a set of additional experimentally measured default parameters (Table 2.1). Quantum frequency conversion can also be modelled within this device, if indicated. After simulating idling, this class returns the fidelity of entanglement after noisy storage.

Distributing Multiple Entangled Pairs: Additionally, entanglement purification can be simulated, which requires distributing N input qubits. This methodology mirrors the single pair case, but the transmission must be updated; rather than waiting for one pair, the memories must wait for N pairs. The noisy storage fidelity is then inputted to the purification class, such as the Multi-Copy Nested protocol (Section 3.7.2), which returns the final probability of entanglement distribution and fidelity after transmission, quantum memory idling, and error correction.

In the quantum error correction module, these two classes of quantum error correction codes are applicable to both quantum channels and quantum memories: in channels, they raise the BSM success probability and thereby reduce the quantum bit error rate (QBER); in memories, they extend the achievable storage lifetime.

3.9 Limitations of QUANTA

Lack of Time-Domain Simulation (JS): To simplify the analysis and computational complexity, the simulation of the time-domain has been omitted. Experimentally, a minimum coincidence rate $R_{\min} > 0$ is caused by the accidental count rate $R_{\text{acc}} \approx S_A S_B \tau_{\text{coinc}}$, where $S_{A,B}$ is the photon detection rate of detectors A or B, which includes accidental detections from unpaired photons and dark counts [77]. If time was simulated, single photon detection events at each detector would be timestamped, and the maximum and minimum $g^{(2)}(\tau)$ cross-correlation functions between detection events would be computed. A coincidence window can be chosen to encompass the entire jitter distribution to maximize entanglement distribution rate or a smaller window about $\tau = 0$ to prioritize visibility. The timing agnostic simulator can still model the visibility of noisy sources and detectors with the provided assumptions; however, it is not possible to characterize synchronisation issues such as clock drift between nodes or temporal overlap between interfering photons within their mutual coherence time at a BSM [77]. The simulator assumes operations are always synchronous.

Quantum Memory Maximum Idle Time (CM, JS): Section 3.5 describes how time-dependent noise is applied to idling qubits as defined by recent work. To simplify modelling and analysis, QUANTA assumes that once a qubit has idled for the maximum storage time τ_s , it becomes unrecoverable, and both fidelity and distribution rate drop to zero. In practice, this is unrealistic because stored states undergo a gradual, exponential loss of coherence as a function of storage time [30], [78].

Practical Challenges Implementing EP Protocols (Section 3.7.2) (JMa): In the multi-copy [72], nested EP scheme, a large number of qubits must be provided concurrently, which in turn requires substantial quantum-memory resources to buffer these qubits. In the polarization–frequency (Pol–Fre) hyperentanglement scheme [73], the hardware must be capable of generating single photons hyperentangled across polarization and frequency. Our platform presently lacks such a source, and therefore the Pol–Fre hyperentanglement protocol cannot be fully realized in the current system.

3.10 Comparing QUANTA with Other Quantum Network Simulators (JS):

QUANTA prioritises flexible hardware modelling and minimal computational overhead to simulate both single links and repeater chain networks. By easily configuring link device parameters, the effect of future device performance on network performance can be estimated with QUANTA. Or, the minimum device performance necessary to meet some network performance requirement can be investigated. This estimation procedure is computationally efficient as calculations are analytical.

Within the Physical layer of the network stack [79], QUANTA is limited to only two predefined single link architectures (Section 3.2) and only one predefined repeater chain architecture (Section 3.3). This design decision was made to prioritize completeness and accuracy within the report’s time constraints. Extending QUANTA to support more flexible interfacing of components requires the simulation of time between components and more detailed qubit representations. Beukers provide the QuREBB framework [53] simulating time-aware single links with configurable qubit encodings, atomic emission platforms, quantum memory platforms, BSMs with ancillary qubits, and link architectures. While Beukers provides more flexible single link hardware configurations, QUANTA would be indicated for hardware analysis of single repeater chains and networks within the supported architecture.

Simulating network layers above the Physical layer requires support for many links, nodes, and protocols running on these nodes [79]. This complexity often results in the simulators of these layers, such as NetSquid [80] or SeQUENCe [81], employing discrete-event simulation to abstract the modelling of qubit encodings and network hardware to simplify the software implementation and user interfacing. Event-based simulators also require higher computational overhead than analytical ones. QUANTA provides a trade-off between simulators like QuREBB [53] and NetSquid [80] by enabling the efficient simulation of a hardware-aware repeater chain networks while restricted to a single architecture.

4 Results

4.1 Single Link Hardware Characterization (JS, JMc)

Using the analytical methods described in Section 3.2.3, the performance of both links as function of total link length L is reported in Fig. 4.1. The link is assumed to utilize a single wavelength channel in the C-band.

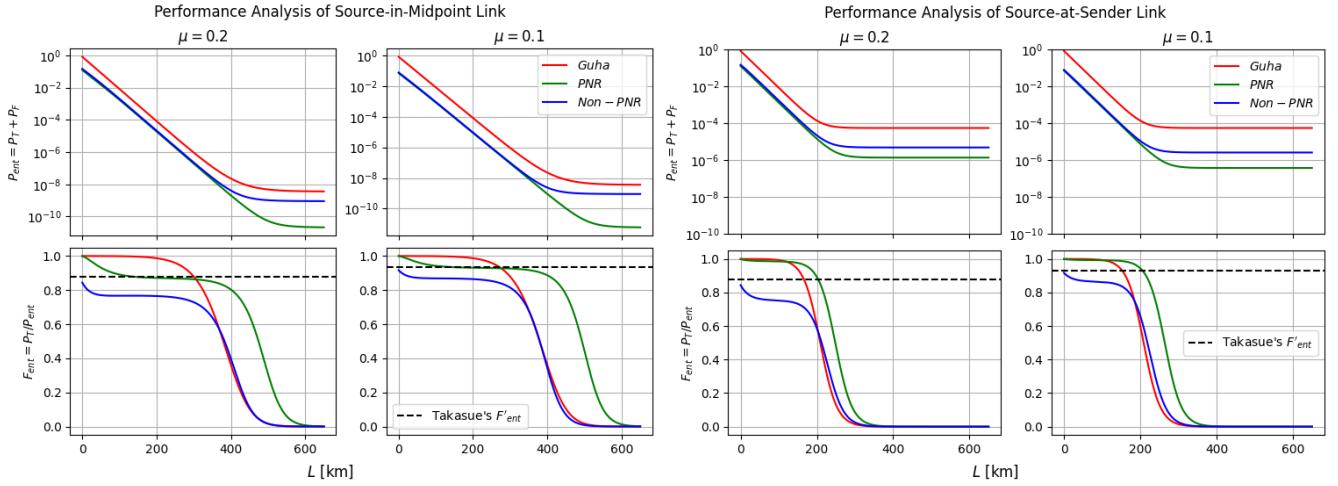


Figure 4.1: Single Link characterization: Probability of entanglement distribution and fidelity vs. link length L using a single C-band channel. Compares Guha’s [1] model with realistic sources and detectors described by Takasue and Clark [3], [4]. Parameters configured as $R_{rep} = 50$ MHz, $x = 100$ emitted pairs, $\alpha = 0.2$ [dB/km], $\eta_d = 0.9$, $P_{DC} = 3 * 10^{-5}$ [1], [3], [14], [17], [82].

Midpoint Distribution Rate: The P_{ent} distributions demonstrate that Guha’s deterministic source predicts higher entanglement distribution rates versus realistic sources. While deterministic sources will always successfully distribute entanglement at perfect transmission, links with non-deterministic sources have $P_{ent} \propto \mu$ [3]. At perfect transmission, non-PNR detectors have $P_{ent} \simeq P_{em}(\mu = 0.2, x = 100) = 0.174$ and $P_{ent} \simeq P_{em}(\mu = 0.1, x = 100) \simeq 0.0930$. PNR detectors are slightly lower than this value since they omit multi-pair detection events. At effectively $\eta \approx 0$, P_{ent} is lower-bounded by dark counts producing the correct heralding pattern.

Midpoint Fidelity: As expected, Fig. 4.1 demonstrates $F_{ent} \propto \frac{1}{\mu}$ [3]. Guha’s fidelity is significantly higher than other configurations since it does not consider the effects of multi-pair emission and detection. Using PNR detectors at perfect transmission and no dark counts, $F_{ent} = 1$ since the $x = 1$ pair will always be transmitted, and any multi-pair detection events are omitted. Non-PNR detectors cannot filter these multi-pair detections, increasing false heralds and decreasing F_{ent} . However, $P_{DC} > 0$ will decrease F_{ent} of Guha’s and PNR detector links from unity at perfect transmission. At $\eta \approx 0$, F_{ent} approaches 0 since effectively no pairs are transmitted.

To verify the simulator’s results, Takasue’s [3] approximation of indistinguishable photon visibility at perfect transmission is plotted. They estimate $V'_{ent} \simeq \frac{\mu+2}{3\mu+2}$, and the corresponding F'_{ent} from Eq. 2.4 is plotted to verify the results of the non-PNR case. Takasue [3] provide this estimation by approximating the non-PNR click probability $P_{click} = 1 - (1 - \eta)^x \simeq x\eta$, meaning the probability of detecting at least one photon is approximately equal to the probability of detecting every photon generated [3]. For a PNR detector, this is true for small but non-zero $\eta \approx 0.01$, verifying this fidelity near $L = 200$ km. The PNR configuration’s fidelity is notably higher than Guha’s for moderate transmission since it can filter some multi-pair detections between real photons and dark counts. As transmission worsens, Guha’s fidelity will be affected by dark counts more quickly.

Source-at-Sender Comparison: Fig. 4.1 reports the performance of a Source-at-Sender link with the same parameters. The performance differences stem from only one photon propagating. At high transmission, the fidelity of PNR detectors is significantly higher than the midpoint configuration, due to the sender’s efficiency staying constant at η_{det} therefore a lower probability of false heralds. The Source-at-Sender architecture provides higher performance relative to the midpoint source at

high to moderate transmission, while trading lower performance at low transmission due to higher attenuation, as the midpoint configuration has two fibres of length $L/2$ and the source-at-sender has a single fibre of length L . This trade-off provides the motivation for Guha's repeater architecture utilizing two Source-at-Sender link's swapping at a midpoint, as they operate in the high to moderate transmission regime.

4.2 Characterization of Swapping Schemes (ZX)

As mentioned previously, Guha's Eq. 3.8 has limitations in that it cannot distinguish the performance of different swapping protocols, such as Sequential, Parallel, and Binary Tree schemes shown in Fig 3.8. This section aims to demonstrate how different protocols affect link performance results, utilising the theoretical formulas derived in Section 3.3.3 and presenting the analysis in Section 4.2.1. Additionally, Section 4.2.2 examines under what conditions the Guha binary tree structure with WDM technology can become the optimal solution.

4.2.1 Analysis of Three General Swapping Schemes

Using the analytical methods described in Section 3.3.3, the raw key rate performance of the Sequential, Binary Tree (full-memory), and Parallel swapping schemes are compared under different single-link transmission probabilities $\eta_{tr} \in \{0.9, 0.6, 0.3, 0.01\}$, as shown in Fig. 4.2.

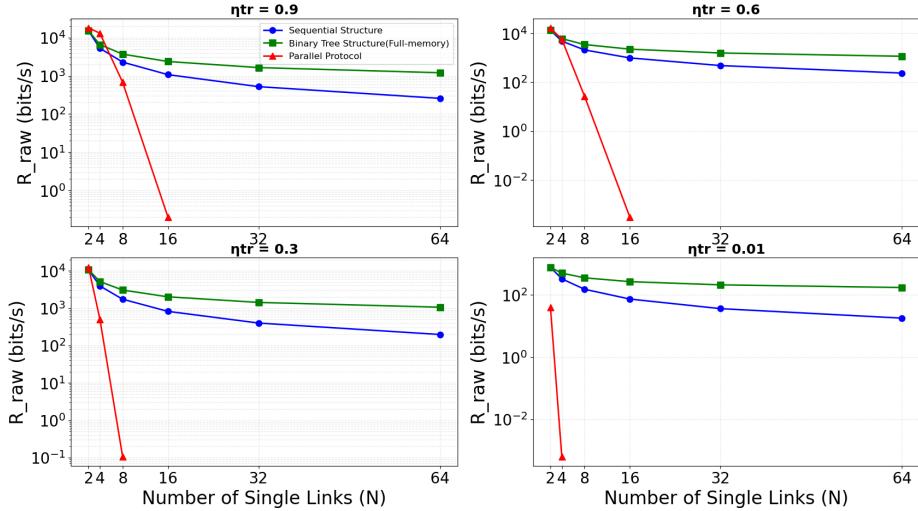


Figure 4.2: The R_{raw} Comparison : Sequential (Blue) vs. Binary Tree with Full-memory (Green) vs. Parallel Protocol (Red) with different η_{tr} . Using parameters setting: $T_q = 1 \mu s$, $\eta_d = 0.8$, $\eta_m = 0.7$, $t_b = 1 \mu s$, $t_c = 20 \mu s$.

The Binary Tree (Full-memory) protocol demonstrates the best scalability under all tested conditions. Its key advantage lies in the logarithmic scaling property derived from harmonic numbers, enabling it to maintain effective key generation rates even under low transmission efficiency ($\eta_{tr} = 0.01$) and in large-scale networks ($N = 64$). The protocol's memory-assisted waiting mechanism effectively mitigates the exponential decay inherent to parallel operations, exhibiting exceptional robustness under realistic channel loss conditions.

The Parallel protocol is clearly the most sensitive protocol to N and exhibits a distinct dual behaviour. Under high transmission efficiency ($\eta_{tr} = 0.9$) and in small-scale networks ($N \leq 4$), it achieves performance comparable to or even exceeding other protocols. However, as network size increases, it experiences an abrupt performance collapse due to the strict requirement for simultaneous entanglement generation across all links. In particular, for $N \geq 16$, the protocol becomes unusable under all tested transmission efficiencies, reflecting its extreme sensitivity to network size.

The Sequential protocol presents a balanced performance profile. In small-scale networks ($N = 2-4$), its performance is close to that of the Binary Tree protocol, but it exhibits a linear degradation pattern as network size increases. This linear decay stems from the cumulative effect of sequential waiting delays, where each additional link segment introduces a fixed time overhead. Unlike the exponential collapse seen in the Parallel protocol, the Sequential protocol's degradation is predictable and relatively moderate. Its main advantage lies in its simplicity of implementation and moderate resource requirements. Compared with the Binary Tree protocol, which demands complex memory management, the Sequential protocol's sequential

processing mechanism is easier to engineer and debug. While its scalability is inferior to that of the Binary Tree protocol, it can still deliver acceptable performance in medium-scale networks ($N = 8\text{--}16$).

These results indicate that the Binary Tree protocol is best suited for large-scale, long-distance quantum network deployments; the Parallel protocol is only suitable for small-scale applications with high-quality channels; and the Sequential protocol can serve as a practical choice for medium-scale networks. This analysis provides an important performance benchmark for selecting protocols in quantum key distribution networks.

4.2.2 Analysis of Two Binary Tree Schemes

Furthermore, in this section, two binary tree scheme will be compared: Guha binary tree and Full Memory binary tree scheme. A WDM strategy will be introduced to enable Guha's structure to outperform the full memory scheme. These are compared by setting

$$T_n^{\text{Guha}} \leq T_n^{\text{Full}} \quad (4.1)$$

according to the analytical equations listed in Appendix 3.3.3. This inequality can be numerically solved for the minimum M^* satisfying:

$$\frac{1}{[1 - (1 - \eta_{tr})M]^2} \leq \frac{3}{2\eta_{tr}} \cdot \frac{1}{\eta_m^2} \quad (4.2)$$

where $1 - (1 - \eta_{tr})^M = \eta_W$ like shows in Eq.2.8. Thus, the Guha scheme outperforms full-memory when:

$$M \geq M^* \quad (4.3)$$

Figures 4.3a and 4.3b show M^* as a function of the link distance D and the single-link success probability η_{tr} , respectively. For short distances (or high η_{tr}), only one or two WDM channels are sufficient. As D increases (or η_{tr} decreases), M^* grows in discrete steps, reflecting the non-linear improvement of η_W with respect to M . A critical jump is observed at $D \approx 100$ km (with $\alpha = 0.20$ dB/km, corresponding to $\eta_{tr} \approx 0.01$, 100 dB channel loss), where M^* increases sharply to 7. Beyond this point, the Guha scheme requires significantly more spectral resources and cost of hardware to maintain its advantage over the full-memory scheme.

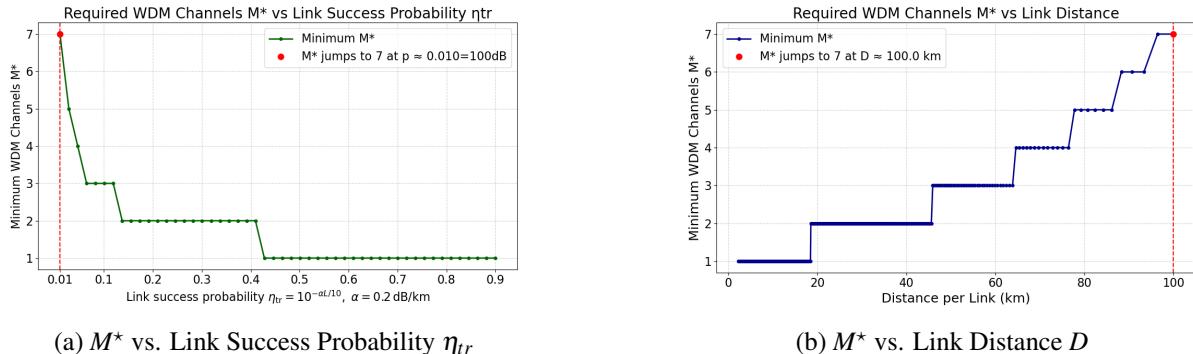


Figure 4.3: Minimum required WDM channels M^* for the Guha scheme to outperform the full-memory binary tree scheme: (a) as a function of single-link success probability η_{tr} ; (b) as a function of link distance D .

These results underscore a practical trade-off shaped by current spectral multiplexing capabilities. Under typical Coarse Wavelength Division Multiplexing (CWDM) technology, which commonly supports at least above 8 wavelength channels in commercially available systems [55], the Guha binary tree architecture can often match or even exceed the performance of the full-memory scheme across a wide range of link distances. This advantage becomes particularly pronounced in moderate-loss regimes, where the required number of WDM channels M^* remains well within the feasible CWDM range.

However, in high-loss scenarios, the spectral demand of the Guha scheme grows rapidly, potentially exceeding the practical channel count provided by standard CWDM systems and necessitating either more advanced Dense Wavelength Division Multiplexing (DWDM) technology or hybrid approaches. Consequently, under present-day WDM constraints, the Guha structure represents a particularly attractive and cost-effective choice for medium-scale quantum networks, where both the

complexity of full-memory management and the spectral overhead of large-scale DWDM deployment can be avoided.

4.3 Trusted Node Chain Characterization(ZX, JMc)

From analytical equation in the Section 3.4 for SKR.Fig. 4.4 compares the effective secret key rate (SKR) in an elementary link (one relay node) predicted by the proposed queueing-theoretic model of Peng [25] with that obtained from the conventional minimum-rate approach [24] as function of the total link distance. Both methods exhibit an exponential decay in SKR with increasing distance, primarily due to fibre attenuation and finite detector efficiency. At long distances ($>150\text{KM}$) the two curves converge, indicating that the SKR is dominated by photon transmission losses and is insensitive to the choice of estimation method.

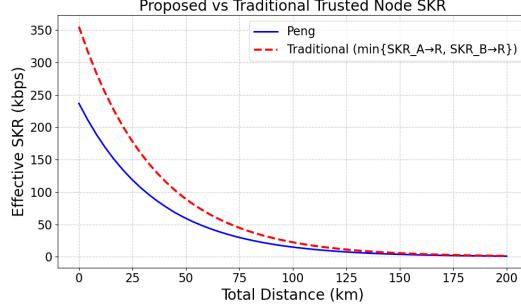


Figure 4.4: SKR Comparison of two scheme in the elementary link. With the assumed parameters: $T_q = 1 \times 10^{-6}$ s, $Q_p = 1000$, $M_b = 15$, $C = 500 \times 10^6$ Mbps, $\eta_d = 0.8$, $\alpha = 0.2$ dB/km, $\Delta = 0.5$

However, at short to moderate distances, the conventional approach yields consistently higher SKR values. This overestimation arises from the implicit assumption of perfect temporal synchronization between the two links, neglecting the stochastic mismatch in key generation rates and the finite relay buffer size. In contrast, Peng's model incorporates these effects via a discrete-time birth-death Markov chain, capturing queueing delays and buffer overflow events at the relay. Consequently, it produces a more conservative SKR estimate that better reflects practical performance.

Fig. 4.5a presents the optimal relay count results calculated using Eq. 3.35. It can be observed that for a total distance of 200 km, the optimal number of trusted relays is 11. And Fig. 4.5b compares the multi-relay SKR variation trends between the traditional minimum-segment-rate model and Peng's model over a total distance of 300 km. The traditional model predicts unlimited SKR growth with increasing relay count without decreasing, which is unreasonable from both physical and engineering perspectives, as relay processing delays in practical systems would limit rate enhancement. In contrast, the Peng model exhibits a trend of initial increase followed by decrease and eventual convergence, which better aligns with practical scenarios. This reflects the trade-off between link segmentation benefits and relay processing overhead (potential waiting time at each relay node, which influenced by: buffering size ($Q_p + M_b$), size of packet (Q_p), and classical transmission (C) see[25] for more details), thereby demonstrating superior modeling rationality.

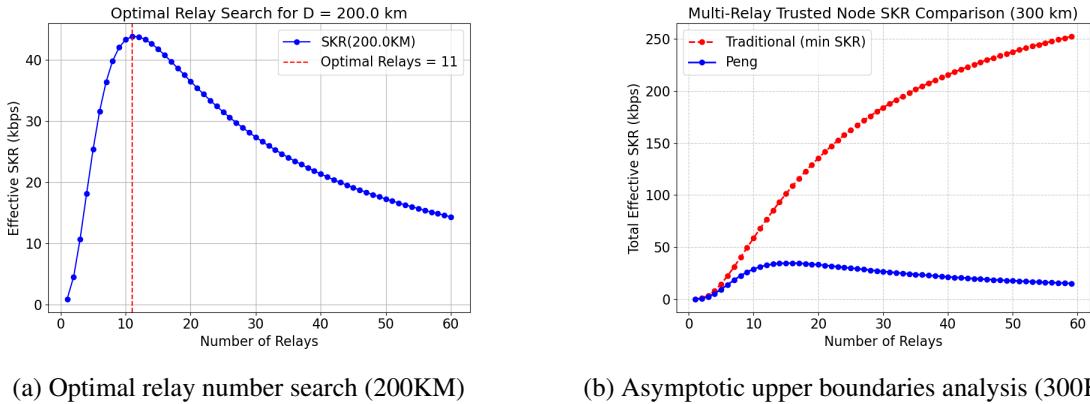


Figure 4.5: Rationality Analysis of the Peng's Model.

4.4 Quantum Error Correction Results (JMa)

Quantum error correction (QEC) is evaluated on lossy optical links and quantum memories using the codes defined in Sec. 3.6. For links, an unencoded baseline is compared with a QPC(5,5) [63] and a GQPC with heterogeneous inner blocks [3,3,3,4,4,4,4] [65], under the same photon budget $N = 25$. For memories, unencoded storage is compared with the five-qubit code [[5, 1, 3]] [67]. Metrics are the logical Bell-state measurement success probability $P_{\text{BSM}}(\eta)$ versus transmission efficiency η and the stored-state survival/fidelity versus time (Figs. 4.6a, 4.6b). Unless otherwise stated, quantum memory defaults are $C = 3$, $\tau = 10 \mu\text{s}$, $\gamma = 1/100 \mu\text{s}^{-1}$, $\gamma_s = 1/50 \mu\text{s}^{-1}$, and $T \in [0, 1000] \mu\text{s}$.

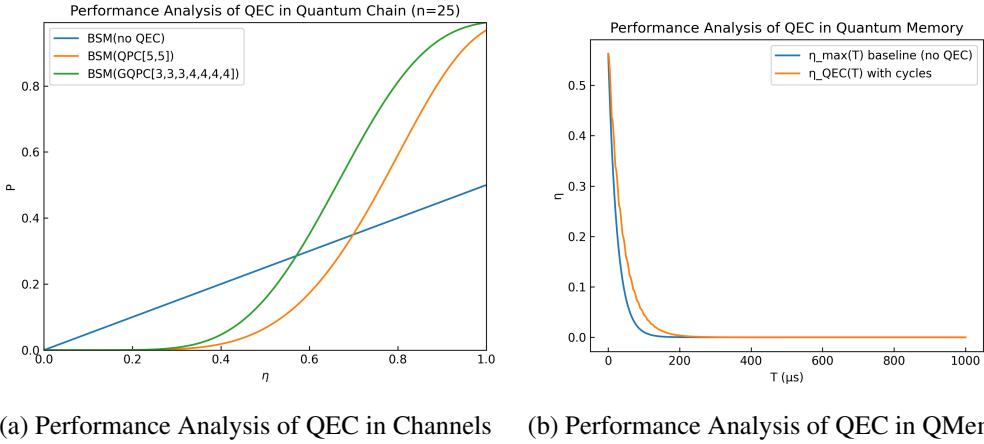


Figure 4.6: Analysis of Quantum Error-Correcting Codes Performance

On lossy links, both parity codes substantially increase P_{BSM} over the unencoded case across practical η . For fixed N , GQPC consistently surpasses QPC by exploiting non-uniform inner-code lengths to better convert surviving photons into a logical success, yielding higher P_{BSM} especially at moderate–high η (Fig. 4.6a), consistent with parity-code BSM theory and the generalized design’s resource efficiency [63], [65]. In QKD terms, higher P_{BSM} directly boosts entanglement yield per attempt and thus increases secret-key throughput at fixed QBER (see Sec. 4.7).

For quantum memories, the five-qubit [[5, 1, 3]] code with periodic syndrome extraction markedly extends effective coherence: at a given dwell time, the encoded logical qubit exhibits a higher survival probability than the unencoded one; equivalently, to meet a target fidelity threshold, the encoded case tolerates a longer storage interval (Fig. 4.6b). As long as error events remain sparse (no more than one per correction cycle), single-qubit errors are detected and corrected [67], stabilizing storage during multi-hop setup and classical signaling.

In summary, GQPC on links (higher loss tolerance and P_{BSM}) and the five-qubit codex in memories (prolonged retention) are complementary, jointly enhancing end-to-end entanglement distribution and secret-key rates under realistic device and channel conditions.

4.5 Performance Analysis of Entanglement Purification Module (JMa)

This section evaluates entanglement purification (EP) protocols and auxiliary modules under unified assumptions and consistent metrics. Unless specified otherwise, measurements are ideal. For the polarization–frequency (Pol–Fre) hyperentanglement protocol, the external conversion efficiency is fixed at $\eta = 0.57$, with Scenario 1 using $(B, C) = (0.60, 0.40)$ and Scenario 3 using $(A, B, C) = (0.40, 0.30, 0.30)$. Comparative results are reported in terms of output fidelity F_{out} , success probability P_{succ} , resource consumption, and the composite index R .

4.5.1 Protocol- and Module-Level Performance

Protocols and functional modules from Sec. 3.7 were evaluated under the unified settings above. For the measurement-based purification module, identical measurement noise is assumed at both ends with the same number of ancillary qubits $n = m$; the case $n = 1$ corresponds to the no-purification baseline.

Figs. 4.7a and 4.7b show that, for both Nested DEJMPS and Multi-Copy Nested, shallow nesting achieves superior performance at high input fidelity F_{in} , whereas deeper nesting is advantageous only at lower F_{in} . The mechanism is the rapidly

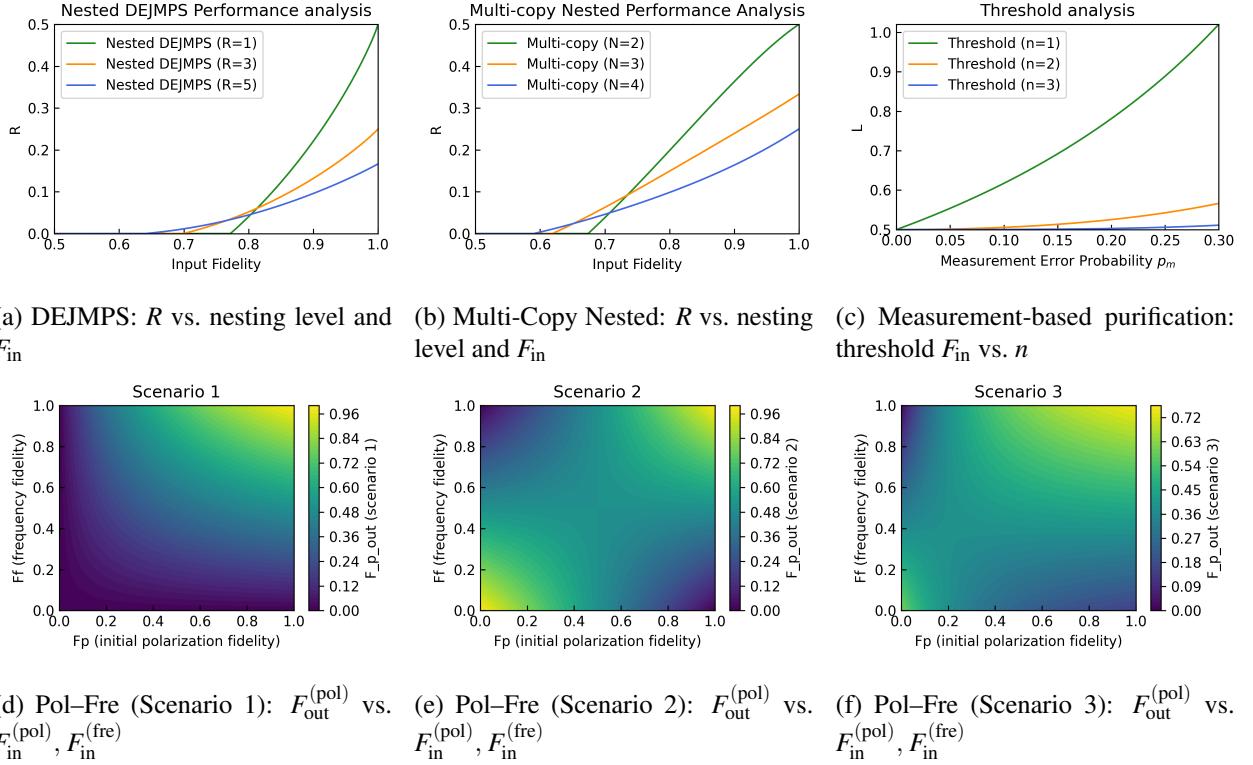


Figure 4.7: Protocol- and module-level performance under unified assumptions.

increasing resource consumption with nesting depth, which reduces overall efficiency—and thus the composite index R —in the high- F_{in} regime despite marginal gains in F_{out} [72]. Across the Pol–Fre hyperentanglement protocol (Figs. 4.7d–4.7f), the output polarization fidelity increases monotonically with the input polarization fidelity; a higher input frequency fidelity further enhances the purification effect. Scenario 1 exhibits the strongest improvement, while Scenarios 2–3 are moderate [73]. The measurement-based purification module (Fig. 4.7c) lowers the minimum input-fidelity threshold required for net improvement; by $n = 3$, the impact of measurement noise on this threshold is negligible, consistent with recent analyses of purifying noisy local measurements with small ancilla overhead [68].

4.5.2 Aggregate Comparison Across Protocols

A unified comparison over F_{out} , P_{succ} , resource consumption, and R was performed with no measurement noise, no measurement-based purification, and no reset-and-reuse. The nesting depth for Nested DEJMPS and Multi-Copy Nested was set to two rounds; for Pol–Fre hyperentanglement, $\eta = 0.57$ and the above error scenarios were used.

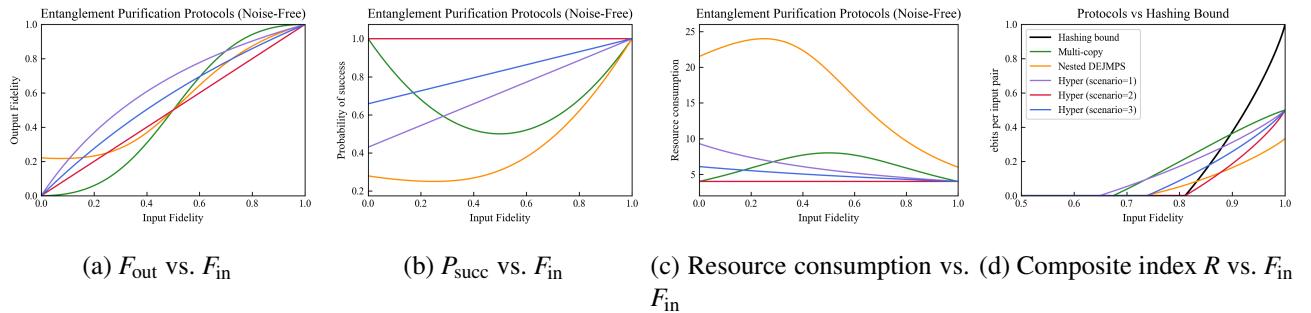


Figure 4.8: Aggregate comparison across protocols under unified settings.

Under these conditions, each protocol presents distinct strengths as a function of F_{in} : nested schemes trade higher resource consumption and reduced P_{succ} for fidelity boosts at lower F_{in} , while the single-pair hyperentanglement scheme attains large

fidelity gains with high yield provided the auxiliary degree of freedom and conversion are of sufficient quality [68], [72], [73]. In practice, the simulator allows systematic tuning of key parameters—such as nesting depth, ancillary-qubit number n , conversion efficiency η , and error composition (A, B, C)—to identify, for a given F_{in} and device constraints, the entanglement purification strategy that best meets a target objective (e.g., maximizing R or jointly optimizing F_{out} and P_{succ}).

4.6 Performance Analysis of Repeater Chains (All)

4.6.1 Repeater Chains with Perfect QM (JS, JMc)

Utilizing the methods described in Section 3.3.2, the performance of repeater chains performing Parallel swapping are investigated as function of their EL number, N_e . Each EL utilizes current generation DWDM hardware supporting 50 GHz (0.4 nm) ITU channels to support $M = 85$ wavelength channels in the C-band (1530.33 - 1564.68 nm) [55], [83].

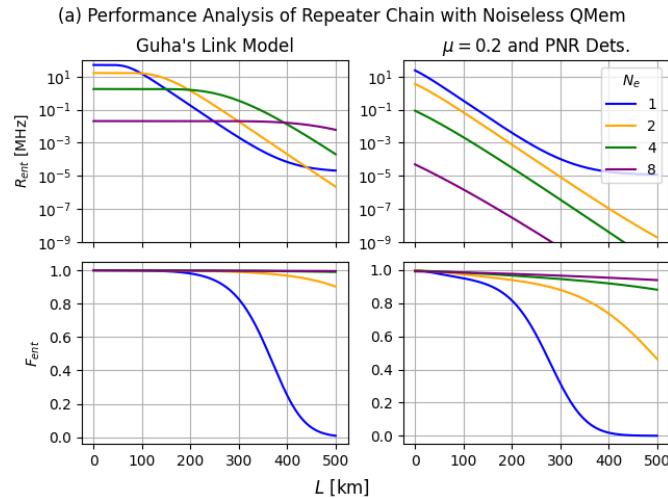


Figure 4.9: Repeater Chain with Parallel Swapping and noiseless QM: Rate of entanglement distribution and fidelity vs. total chain length L . Compares Guha’s [1] model with realistic sources and detectors described by Takasue and Clark [3], [4]. Parameters configured as $M = 85$, $\eta_{\text{load}} = \eta_{\text{emit}} = \eta_d = 0.9$, and all other parameters equal to Fig. 4.1. N_e denotes the number of EL links in a chain.

Guha’s Repeater Chain: Fig. 4.9 characterizes repeater chains utilizing theoretical quantum memories that load and emit qubits with efficiencies η_{write} and η_{read} but impart no noise on the stored state. Guha’s [1] model demonstrates that quantum repeaters with noiseless and deterministic sources are able to outperform single links (i.e. $N_e = 1$) as total link length L increases. There exists an optimal N_e for a certain link distance L to maximize R_{ent} . Without loss of generality, links with lower N_e will be optimal until fibre attenuation begins to dominate as L increases. Incrementing N_e by adding a midpoint repeater station will immediately lower the probability of distribution success as another probabilistic BSM must succeed. However, when L is large and M is high, swapping entanglement at $L/2$ can result in a higher success probability by reducing loss. R_{ent} is lower bounded by the probability of dark counts producing the correct heralding pattern. F_{ent} is always greater with higher N_e as dark count noise and multi-pair effects are minimized with higher transmission.

Repeater Chain with Realistic Devices: When comparing Guha’s [1] idealistic link architecture to links with realistic sources and PNR detectors, Guha’s assumptions result in an overestimate of both R_{ent} and F_{ent} . Critically, this configuration’s R_{ent} with $N_e > 1$ fail to exceed the single link rate. While F_{ent} does increase with N_e , this benefit is erased by R_{ent} always decreasing with N_e . In other words, adding repeater stations does not improve the distribution rate as L increases. This occurs because there are not enough wavelength channels to sufficiently increase the BSM success probability to overcome the loss.

4.6.2 Repeater Chains with Noisy QM and E.P. (JS, CM, JM, ZX, HZ, JMc)

The effects of simulating realistic and noisy Hot-Rb Vapour (Far-off Raman) quantum memories are demonstrated in Fig. 4.10 using the class’s default parameters described in Section 2.3. As noted in Table 2.1, this memory does not interact with wavelengths in the C-band, such as our source device. In this section, the system assumes the existence of perfect frequency conversion to the memories operating wavelength of 795 nm. Inefficient frequency conversion is explored in Section 4.6.4.

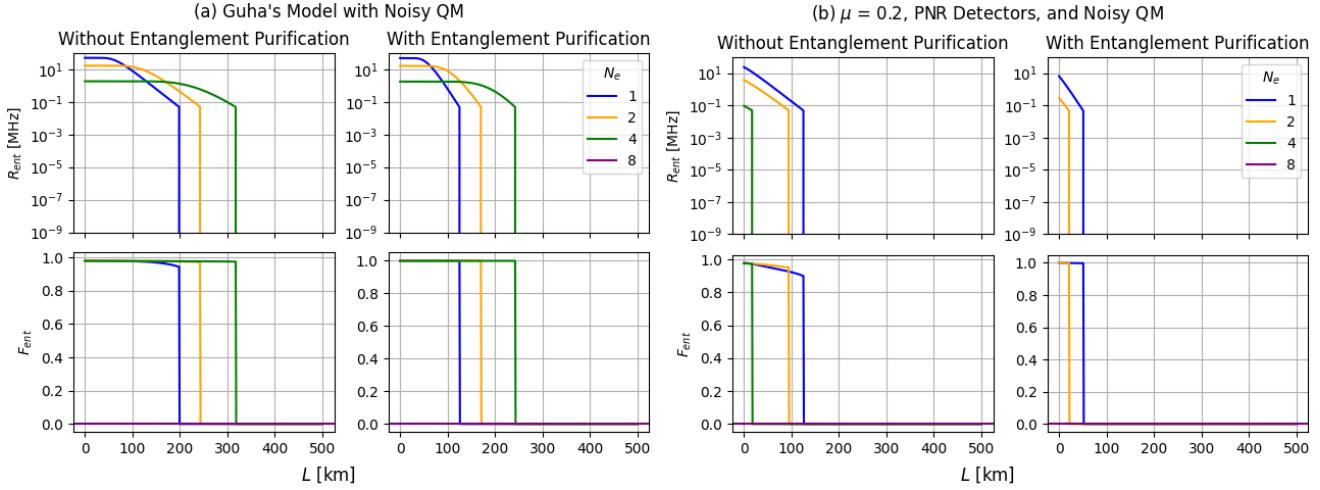


Figure 4.10: Repeater Chain simulating Parallel swapping, Noisy QM, and Multi-Copy Purification: Rate of entanglement distribution and fidelity vs. total chain length L . Compares Guha’s [1] model with realistic sources and detectors described by Takasue and Clark [3], [4]. Parameters configured as $M = 85$, and all other parameters equal to Fig. 4.9. Simulates a Rb Vapour Raman QM with default parameters. N_e the number of EL links in a chain. The simulation assumes qubit is unrecoverable after idling for the maximum idle time τ_s .

As discussed in Section 3.3.3, the expected time in memory for Guha’s repeater architecture is derivable as $1/R_{ent}$ [1], which is then simulated using the RbVapourRaman subclass of the QuantumMemory class to apply the time-dependent noise. The most critical memory parameter is the experimentally characterized maximum time in memory, which is $21 \mu\text{s}$ for this memory type. After a qubit has idled for this time, QUANTA assumes the qubit is unrecoverable so the fidelity and effective distribution rate drops to 0. Maximum time in memory becomes the limiting factor for chain design, and for this configuration, $N_e = 3$ is the maximum possible number of EL. $N_e > 3$ will result in an expected idle time greater than the maximum time in memory for all L . EP is investigated using the Multi-Copy Purify protocol with two input qubits, which boosts fidelity while lowering R_{ent} since it requires the distribution of two qubits. As expected, the performance of realistic hardware in Fig. 4.10(b) has only worsened in comparison to Fig. 4.9(b), apart from a slight boost in purified entanglement fidelity at low loss.

4.6.3 Estimating Repeater Chain Performance with Increased ITU Channels (JS)

The results of Sections 4.6.1 and 4.6.2 indicate that it is necessary to increase the number of multiplexed channels to realize a functioning repeater chain with realistic hardware devices. Recent DWDM and Ultra-Dense WDM (UDWDM) devices have demonstrated ITU channel spacings as small as 12.5 GHz (0.1 nm) [55]–[57]. If the available ITU grid is also expanded to include the L, C, and S-bands, this enables the utilization of significantly more ITU channels. An ITU grid from 1465 - 1565 nm could be selected to maintain an approximately equal attenuation rate of $\alpha \approx 0.2$ [dB/km] across channels [6], which would provide access of up to 1000 ITU channels with 0.1 nm spacing. Fig. 4.11 investigates the performance of repeater chain utilizing noisy sources, PNR detectors, $M = 1000$, and the Parallel swapping scheme.

With this increased number of ITU channels, the realistic hardware functions as a repeater chain where there exists an optimal N_e for each L . R_{ent} increases with N_e for all L until reaching the maximum chain length, albeit a small increase. The model suggests that increasing the number of ITU channels is solely responsible for sufficiently increasing the probability of BSM success to mitigate high transmission loss. With constant M , the distribution is unchanged when the maximum time in memory is increased. A longer time in memory only increases the maximum L of the chain.

4.6.4 Comparison of QM Platforms in Repeater Chains (JS, CM)

Maximum Chain Length: The results of Fig. 4.11 can be compared with every QM supported by the simulator. The performance of these memories using Parallel swapping with both Guha’s link assumptions and realistic link hardware are compared in Table 4.1, with the latter configured with the same link device parameters as Fig. 4.11. As discussed in Section 2.4, the QMs are integrated with QFC devices with associated device and frequency conversion efficiencies. Device transmission

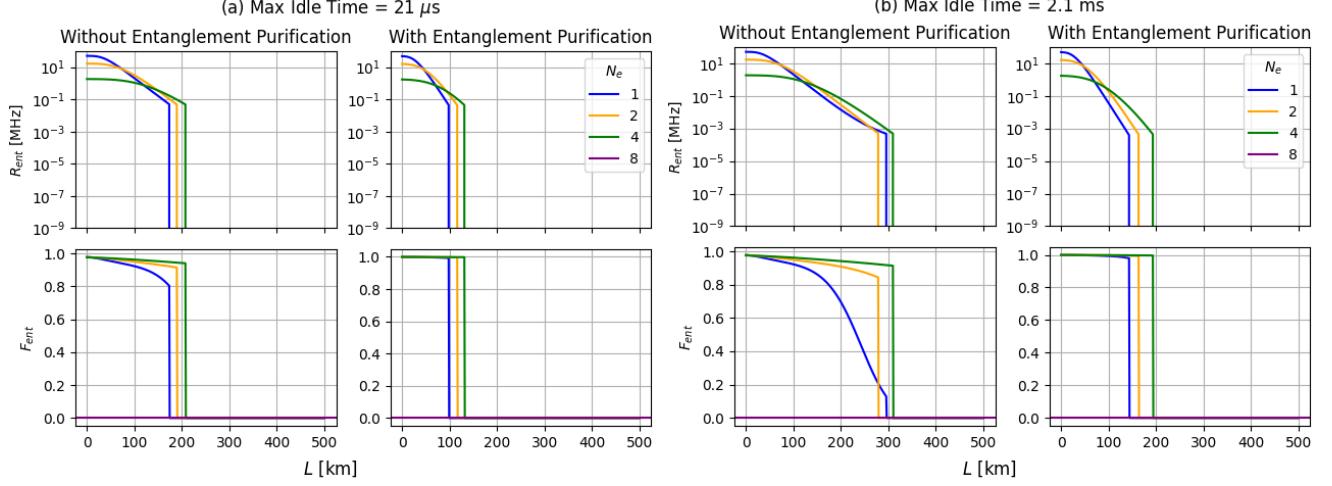


Figure 4.11: Repeater Chain simulating Noisy QM and Entanglement Purification characterization: Rate of entanglement distribution and fidelity vs. total chain length L . Compares performance of realistic sources [3] and PNR detectors [4] when maximum idle time is increased. Parameters configured with $\mu = 0.2$, $M = 1000$, and all other parameters equal to Fig. 4.10. Simulates a Rb Vapour Raman QM with default parameters. N_e the number of EL links in a chain. The simulation assumes qubit is unrecoverable after idling for the maximum idle time τ_s .

efficiency η_{trans} is assumed to be 0.77 for all memory platforms, and the platform specific frequency conversion efficiency is listed in the table as η_{qfc} [36], [37]. The total memory-QFC efficiency is $\eta_{qm-qfc} = \eta_{trans}\eta_{qm}\eta_{qfc}$. The table investigates the performance of the longest possible chain of length L_{max} before qubit idle time reaches τ_s . N_{e-opt} indicates the optimal number of EL needed to reach this maximum distance. R_{ent} and F_{ent} indicate these performance metrics of a chain with length L_{max} .

Platform-Protocol	η_{qm}	τ_s	T [K]	λ [nm]	η_{qfc}	N_{e-opt}	L_{max} [km]	R_{ent} [MHz]	F_{ent}
Er^{3+} Crystal-AFC ^a	0.22	660 ns	1.5	1536	-	(2, 1)	(267, 99.2)	1.54	(0.973, 0.898)
Rb Vapour-EIT ^a	0.67	100 ns	368	795	0.136	(2, 1)	(232, 74.2)	10.2	(0.936, 0.902)
Rb Vapour-Raman ^b	0.82	1.1 μ s	351.7	795	0.136	(4, 2)	(469, 148)	0.916	(0.932, 0.901)
Eu^{3+} Crystal-AFC ^a	0.1	21 μ s	3.5	580	0.245	(2, 1)	(325, 149)	0.0864	(0.927, 0.765)
Pr^{3+} Crystal-GEM ^a	0.69	1.2 ms	3	606	0.245	(8, 4)	(976, 319)	0.000836	(0.922, 0.880)

Table 4.1: Repeater Chain Performance with (Guha, Realistic Link Devices) by QM Platform. Investigates the performance of the longest possible chain of length L_{max} before qubit idle time reaches τ_s . N_{e-opt} indicates the optimal number of EL needed to reach this maximum distance. R_{ent} and F_{ent} indicate these performance metrics of a chain with length L_{max} . Realistic device parameters are equal to Fig. 4.11. References *a*: [28], *b*: [35]

The results demonstrate that even with $M = 1000$ ITU channels, current generation link hardware significantly diminishes link performance across all metrics, except R_{ent} . Thomas [8] highlight the necessary visibility to violate the Bell-inequality as $V_{ent} = 0.707$, which corresponds to a minimum $F_{ent} = 0.780$ by Eq. 2.4. Critically, all configurations, excluding cold Eu^{3+} QM with noisy link devices, achieve this minimum fidelity requirement and are capable of supporting entanglement-based applications, albeit with a low distribution rate. R_{ent} is constant between the link hardware models because the noisy link rate distribution retains the same trend as Guha's but is compressed along the x-axis, L ; both models share the same τ_s which corresponds to the same maximum R_{ent} but at different L_{max} . Future improvements to increase the η_{qm-qfc} and τ_s of QM will increase both storage fidelity and achievable L_{max} , respectively.

The results are consistent with the swapping comparison in Section 4.2.1, which shows that repeater chains using the

Parallel scheme are only viable for small networks with $N_e \leq 4$. The Pr^{3+} platform, however, can exceed this limit thanks to its millisecond-scale τ_s , which supports longer idle times while awaiting successful swapping operations. This aligns with the literature, which emphasises that storage times on the order of milliseconds are required to surpass the direct transmission distance limit [27]. The Eu^{3+} platform displays the opposite effect, where the optimal N_e is not the maximum supported EL due to having the lowest QM efficiency. This decreases the swapping success probability as qubits are loaded and emitted from QM with a lower probability; qubits idle too long with higher N_e while waiting for all more swaps to succeed. Future work should investigate the performance of competing swapping schemes (Section 4.2).

Minimum Idle Time in Memory: Table 4.1 indicates the only memory platform in the C-band, Er^{3+} Crystal, has the best distribution rate and fidelity. This is partly because it has the highest overall efficiency, as it does not require frequency conversion. Its operating wavelength makes it a suitable candidate for another investigation regarding the minimum memory idle time τ_s necessary to achieve a repeater chain of length L with an optimal number of EL, N_{e-opt} . Table 4.2 reports the minimum τ_s necessary to achieve a repeater chain of length L with Er^{3+} Crystal memories. L is selected to be further than the L_{max} achieved with this device's current τ_s in Table 4.1. Multiple EL link numbers are tested, and the table reports the smallest N_e that provides a $F_{ent} > 0.707$ [8]. As expected, the minimum required memory time increases significantly with distance. The fidelity behaviour needs further explanation, as it does not consistently decrease. This results from the N_{e-opt} selection criteria. For $L = 300$, if N_e was chosen to be 4, the fidelity would be higher than at 400 km as fidelity increases with transmission. However, $N_e = 2$ provides higher a higher distribution rate while still violating the Bell-inequality.

L	τ_{s-min}	N_{e-opt}	R_{ent} [MHz]	F_{ent}
200	0.279 ms	2	0.00359	0.880
300	0.0227 s	2	$4.40 * 10^{-5}$	0.788
400	43.6 s	4	$2.29 * 10^{-8}$	0.846

Table 4.2: Repeater Chain Performance using RE Crystal (Er^{3+}) with realistic device parameters equal to Fig. 4.11. Investigates the minimum τ_s necessary to achieve a total repeater chain length of L . N_{e-opt} indicates the optimal number of EL to reach this minimum idle time. R_{ent} and F_{ent} indicate these performance metrics at L .

4.6.5 Entangled Network Resource Allocation (JS, CM, JMa, JM_c, HZ, ZX)

Within entangled networks, repeater chain resources may be shared unequally across different elementary links. These chains may also have nodes with degrees greater than two and more than one user per end-node. Illiano [79] provide a comprehensive survey of the quantum Internet's protocol stack, inspired by the classical TCP/IP hierarchy. They define the distribution of entanglement between two directly connected nodes as a physical entanglement connection, which can be swapped within an interior network node to entangle two nodes that do not share a direct link, denoted a virtual entanglement connection. Guha's [1] wavelength-multiplexed links are capable of allocating wavelength channels depending on available hardware resources and performance requirements between nodes. This also enables the existence of multiple network users on a single node.

To investigate the rate of virtual link generation, the network in Fig. 4.12(a) is simulated utilizing noisy sources and PNR detectors. Each link in the figure is an elementary link, and each end-to-end path is a repeater chain with $N_e = 3$. Each link is assumed to have M available wavelength channels and quantum memory positions at each node. Entanglement is distributed and swapped to form virtual connections between the following user pairs: $A - C$, $B - C$, $D - E$. The number of wavelength channels and quantum memory positions are then equally allocated to each virtual connection. For example, all three connections utilize the link connecting both interior nodes, so the available channels per connection is $M/3$.

The network is simulated with each elementary link's $L = 50$ [km], $\mu = 0.2$, $\alpha = 0.2$, and all other parameters equal to Fig. 4.11(a). The three virtual links are compared with and without entanglement purification using Multi-Copy Purify protocol consuming two input qubits. Since all virtual connections have equal transmission and P_{DC} , they have equal fidelities. Without purification, all connections have a $F_{ent} = 0.9569$, while purification provides a higher $F_{ent} = 0.9978$ at the expense of a lower R_{ent} . Since entanglement distribution and swapping are attempted on multiple wavelengths, if sufficient wavelengths are used, R_{ent} can exceed the maximum probability of a 3 node path succeeding at $L = 0$ [km] with $M = 1$. Each BSM succeeds with a maximum probability of $\frac{1}{2}$ using one wavelength channel. For 5 BSMs utilizing one wavelength channel at $L = 0$ [km], this

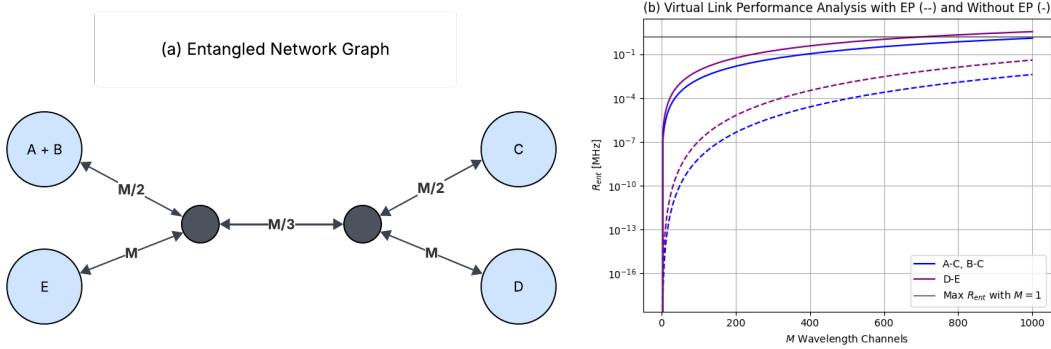


Figure 4.12: (a) Simulated entangled network with connections between nodes $A - C$, $B - C$, and $D - E$. Link subscripts denote the number of wavelengths allocated per connection. (b) Virtual link performance as function of wavelength channels allocated.

maximum probability is $P_{succ} = 0.5^5$, which corresponds to a maximum $R_{ent} = R_{rep}P_{succ} = 1.5625$ [MHz].

4.7 Performance Analysis of Quantum Key Distribution (HZ)

Performance modeling of quantum key distribution (QKD) is performed for three representative architectures: single link, repeater chain, and mesh network according to the E91 protocol[38], [84]–[87]. The analysis focuses on the quantum bit error rate (QBER) and the secret key rate as primary metrics. For each architecture, physical effects including channel transmission efficiency, multipair emission probability, and detector imperfections are incorporated into the model. The comparative evaluation quantifies architecture-level trade-offs and yields parameterized outputs suitable for integration into a quantum-network simulator. These models constitute the system link-level performance module, designed to interface with higher-layer networking functions.

In this protocol, entangled photon pairs are generated at a source and distributed to two parties. Local measurements were performed on the received photons to obtain highly correlated bit values, which were then processed to establish a shared secret key. The primary performance metrics considered in this modeling are the QBER and the secret key rate, both influenced by several physical parameters in practical systems. At the link level, photon loss, absorption, and scattering is characterized by transmission efficiency η_{tr} (2.7).

However, the dark count probability accounts for noise-induced detector clicks. The reliability parameters for BSM in entanglement swapping are incorporated for more complex scenarios. The secret key rate is then determined from the QBER using:

$$P(Q) = 1 - 2h_2(Q), \quad (4.4)$$

where $h_2(Q)$ is the binary entropy function [88], [89].

4.7.1 Performance Analysis of QKD in Single Link

A single-link quantum network consists of two end nodes connected by a direct optical channel, with an entangled-photon source located either at one end or at the midpoint. Photons travel along the channel to each node for measurement in the chosen bases. The topology contains no intermediate stations, representing the simplest configuration and forming the basic unit from which larger quantum network architectures are constructed. For an elementary link in an entanglement-based QKD system, the asymptotic secret-key rate per unit time is expressed as

$$R = \frac{1}{2T_q} P_{succ} P_{sift} R_2(Q), \quad (4.5)$$

In this expression, T_q denotes the time interval per experiment, the interval from the beginning of an elementary link test to the system being ready to start the next test. The factor P_{succ} denotes the heralded probability that the elementary entangled link is successfully established in the given trial and is determined by source emission statistics, transmission losses on both half-

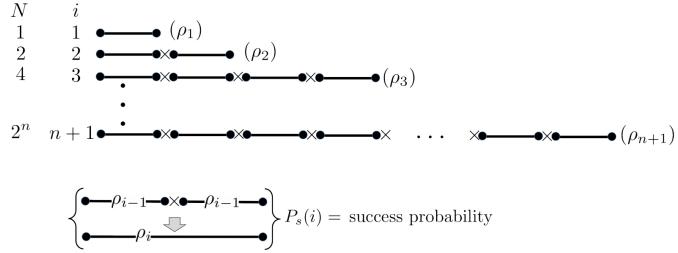


Figure 4.13: Example of possible $N=2^n$ elementary link connections. Adapted from Guha Fig. 2 [1].

links, and BSM detection efficiencies employed at the link center. The term P_{sift} represents the sift probability, the probability that both remote parties choose the same measurement basis and obtain detection resultsthat are kept for key processing[1].

The quantum bit error rate (QBER) Q_1 for the elementary link is obtained from the joint detection statistics and accounts for intrinsic misalignment errors as well as spurious detection events such as detector dark counts. In compact operational form, the QBER is written as a ratio of erroneous coincidence probability to sifted coincidence probability.

$$Q_1 = \frac{P_{\text{err}}}{P_{\text{click}}} \quad (4.6)$$

where P_{click} denotes the probability of a sifted coincidence event (both parties choose the same basis and valid detection clicks are registered within the coincidence window), and P_{err} is the probability that such a sifted event yields an erroneous bit value with respect to the expected correlations. The latter aggregates random errors (e.g. dark-count-induced) and deterministic errors (e.g., polarization/phase misalignment or crosstalk). Using the visibility factors introduced earlier, the same QBER can be written as

$$Q_1 = \frac{1}{2} [1 - t_d t_e] \quad (4.7)$$

where t_d and t_e are dimensionless correlation (visibility) terms that arise from detector alignment and contrast of entanglement. By construction $t_d, t_e \in [0, 1]$, with $t_d = t_e = 1$ corresponding to a perfectly aligned, noise-free link. Substituting (4.6) and (4.4) into (4.5) yields the usable secret-key generation rate for the single elementary link that serves as the performance baseline for multihop constructions.

$$R = \frac{1}{2T_q} P_s(1) P_1 R_2(Q_1). \quad (4.8)$$

Building upon the performance analysis of a single elementary link, the framework can be extended to a chain of multiple links connected through intermediate nodes. In this architecture, entanglement swapping is performed at repeater stations, enabling the distribution of entanglement over distances that far exceed the attenuation length of the optical channel. However, each swap operation introduces additional sources of imperfection, including finite BSM success probability, memory inefficiencies, and cumulative detector noise [38]. As a result, both the overall success probability and the quantum bit error rate (QBER) become functions of the number of segments and the characteristics of each link. While the single-link QBER depends primarily on local misalignment and dark counts, the QBER in a repeater chain evolves recursively, as errors propagate through successive entanglement swaps. This recursive behavior must be explicitly quantified to determine the achievable secret key rate over the entire chain, thus motivating the formulation of the repeater-chain QBER model in the next section.

4.7.2 Performance Analysis of QKD in Repeater Chain

Compared to propagation links with a total distance of L , the quantum network of the relay chain concatenates multiple basic links, and intermediate nodes perform entanglement exchange of qubits emitted from memory. The link is divided by the dichotomy, that is, the number of segments. It is often taken that $N = 2^n$ (to facilitate hierarchical swapping) and the length of each segment $L_0 = L/N$, where n denotes the number of rounds of nested series/entanglement swapping. When a linear chain of $N = 2^n$ identical elementary links is concatenated by repeater nodes that perform Bell state measurements, the end-to-end secret-key rate (per unit time) is obtained by replacing the single link success and QBER terms by their end-to-end counterparts. If the final end-to-end shared state after concatenation of N elementary links is heralded by probability $P_{\text{succ}}^{(\text{end})}$

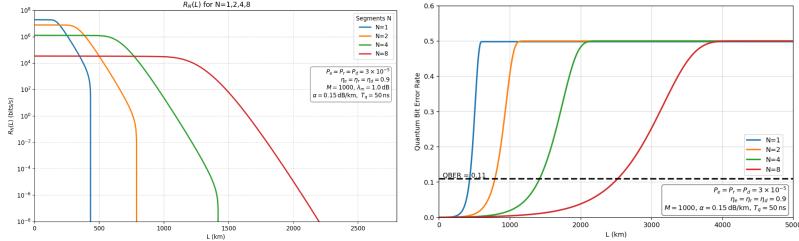


Figure 4.14: QKD and QBER of Repeater Chain with N segments.

and its sifted QBER is Q_N , then the achievable rate becomes:

$$R_N = \frac{1}{2T_q} P_{\text{succ}} P_1 R_2(Q_N). \quad (4.9)$$

The general heralding probability for a chain of N links can be compactly expressed in terms of the per-stage success probabilities P_e (for an elementary link) and P_r (for each repeater connection) as:

$$P_{\text{succ}} = P_r^{N-1} P_e(1)^N, \quad (4.10)$$

which matches the multiplicative structure of independent heralds in the N elementary segments and the $N - 1$ internal connections.

In a repeater chain quantum network, multiple elementary links are connected through intermediate nodes that perform entanglement swapping. Although the physical configuration is more complex, its error behavior can be traced back to the single link case. For a single link, QBER is determined primarily by channel attenuation and drift, detector noise, and source imperfection (multiple pairs are generated, visibility decreases). When extended to a chain, each swapping operation not only preserves part of the existing errors but also introduces the loss of each link and each delay BSM. These effects accumulate in a recursive manner as the number of links increases. Therefore, the QBER formulation for a repeater chain can be viewed as a systematic recursive extension of the single link model, enabling mathematical derivation of error growth and its impact on the final secret key rate. A crucial analytical result concerns the manner in which QBER propagates through successive connection levels. Denoting by Q_i the QBER of the two-qubit state obtained after connecting 2^{i-1} elementary links (so that Q_1 is the elementary link QBER and Q_{n+1} is the end-to-end QBER for $N = 2^n$), an exact recursion was derived:

$$Q_i = \frac{1}{2} \left[1 - \frac{t_d}{t_r} (t_r t_e)^{2^{i-1}} \right], \quad 1 \leq i \leq n+1, \quad (4.11)$$

where $t_e = (1 - 2w_1)/(1 + 2w_1)$, $t_r = (1 - 2w_r)/(1 + 2w_r)$, and $t_d = ((q_1 - q_2)/(q_1 + q_2 + q_3))^2$. The factor t_r/t_d depends only on loss and noise parameters of the repeater-node detectors and the end-point detectors respectively (in particular on their dark count probabilities and detection efficiencies). In the elementary link state ρ_1 , $2w_1 = 2c_e/(a_e + b_e)$ is the relative probability of classical correlations to that of pure Bell states. At each repeater connection, $2w_r = 2c/(a + b)$ is the fractional probability of spillover to the classically correlated states[1]. The functional form (4.11) implies a quadratic worsening (squaring) of the bias Q_i at each connection level, modulated by the detector noise prefactor. Consequently, small deviations from the perfect fidelity at the elementary link can be amplified through concatenation, and the end-to-end QBER can be predicted from the measured elementary link QBER using repeated application of (4.11).

From (4.9) and (4.11), the trade-off between the choice of the number of elementary links N , the detector and memory imperfections, and the achievable long-distance rate can be analyzed.

In the diagram of the result of QKD, the key rate drops exponentially with distance, with higher N values enabling longer transmission distances. For example, $N = 1$ fails beyond 400 km, while $N = 8$ extends key generation up to ~ 2400 km. This gain comes at the cost of reduced key rate at short distances due to additional swapping operations. In the diagram of the result of the QBER derivation, which grows with distance, steeper increases are observed with fewer segments. In particular, all curves cross the QBER threshold of 0.11, beyond which secret-key distillation is no longer possible. The curve for $N = 8$

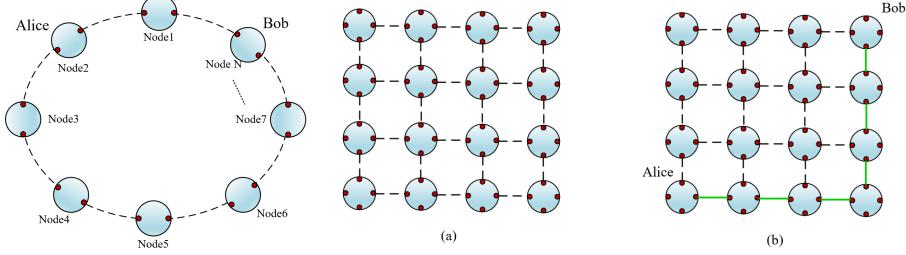


Figure 4.15: (a) Ring and (b) Square Mesh Topology

remains below this threshold longest, aligning with the maximum range of the top plot. Together, the results illustrate the core trade-off: increasing N improves long-distance performance, but reduces the rate in the short range. This guides optimal repeater placement in quantum network deployment.

In the idealized zero dark count limit, the scaling of the optimized rate envelope with total transmittance η was found to follow a sublinear power law $R(\eta) = A\eta^\xi$ with exponent $\xi < 1$, where A is a distance-independent constant prefactor that aggregates device and timing efficiencies (in this model explicitly $A = \eta_d^2/(\eta_r^2\lambda_m^2T_q)$); ξ is the decay exponent, meaning that after optimizing the number of segments N , the key rate scales with the end-to-end transmittance as $R \propto \eta^\xi$ —its “slope” on a log R –log η plot[1], which shows that, under optimal conditions, repeater chains can outperform direct transmission bounds in the loss-limited regime.

4.7.3 Performance Analysis of QKD in Mesh Network

To extend QKD beyond linear repeater chains, a mesh network is introduced so that path diversity, robustness to failures, and traffic engineering can be achieved while reusing the per-link parameters[90], [91] and the QBER recursion developed earlier. Two representative topologies are considered: the ring topology and the square-grid topology [92]. In a ring, each node is connected to exactly two neighbors, forming a closed loop in which entanglement swapping is performed at intermediate nodes. Sources can be placed at midpoints to balance loss, and analytical end-to-end QKD/QBER[1] along any pair of nodes can be computed by composing elementary links. In square-grid topology, nodes are connected to the nearest neighbors on a grid. Benefits include multiple vertex-disjoint shortest paths, load balancing, graceful performance under local failures, and scalability compatible with percolation-style connectivity. Frequency-multiplexed links and memory-assisted swapping can be incorporated locally, while route length and error growth remain analysable with the same single link and repeater chain primitives[93]. These features make ring and lattice suitable baselines for mesh-network evaluation.

Topology of ring quantum networks: The ring quantum network extends the linear repeater chain by connecting its endpoints, forming a closed loop of nodes. Unlike the repeater chain, there are two alternative paths between any pair of nodes, enabling redundancy, load balancing, and potentially improved QKD performance when one path experiences higher loss or noise. A path along the ring consisting of elementary L links (specifically, the shorter arc between Alice and Bob) is considered. For each local elementary link, QBER is denoted as Q_1 , and the quantity a known as bias is by the following:iby the following: by the following:

$$a = P_{\text{agree}} - P_{\text{disagree}} = 1 - 2Q_1 \quad (4.12)$$

a is essentially a quantity within the range of $[-1, 1]$, which can more intuitively reflect the strength and direction of the "quantum correlation". That quantifies the deviation from a random outcome: a value closer to 1 indicates stronger correlation between measurement outcomes, while a value closer to 0 implies randomness. When two paths with biases a and b are connected by a Bell state measurement of linear optics, the resulting bias is of the form: $a' = kab$, where $k = t_r/t_d$ is the repeater/detector noise prefactor. To effectively account for multipair emissions in a phenomenological manner, k is replaced by $c = t_r/t_d - 4p(2)$. Under this correction, the multiplicative connection rule reduces to a well-known symmetric recursion that frequently appears in iterative connection models :

$$a_i + 1 = ka_i^2 \quad (4.13)$$

Using the connection rule above, an inductive closed form for an arbitrary integer path length L is obtained as follows. Suppose

that the path is partitioned into M contiguous subsegments whose lengths sum to L ; let the bias of the j -th subsegment be a_{s_j} . Each subsegment bias can itself be written (by repeated self-connection when needed) as $a_{s_j} = k^{s_j-1} a_1^{s_j}$. When these M subsegments are sequentially connected, $M - 1$ additional multiplicative factors k are introduced. Therefore, the end-to-end bias is:

$$\begin{aligned} a_L &= k^{M-1} \prod_{j=1}^M a_{s_j} = k^{M-1} \prod_{j=1}^M (k^{s_j-1} a_1^{s_j}) \\ &= k^{M-1} k^{\sum_j (s_j-1)} a_1^{\sum_j s_j} = k^{L-1} a_1^L. \end{aligned}$$

Because this expression is independent of the particular partition $\{s_j\}$, it holds for every integer L . Recalling $a_L = 1 - 2Q_L$, the closed-form QBER for an arbitrary path length L is obtained as

$$Q_L = \frac{1}{2} [1 - k^{L-1} (1 - 2Q_1)^L]. \quad (4.14)$$

The heralding (end-to-end success) probability along the same path follows the multiplicative structure of independent elementary and BSM heralds:

$$P_{\text{succ}}^{(L)} = P_s(1)^L P_s^{L-1}, \quad (4.15)$$

where $P_s(1)$ is the probability of the single link heralding and P_s is the probability of BSM success (connection). Consequently, the achievable secret-key rate (per unit time) for the selected path is written in the same Guha-style form:

$$R_L = \frac{1}{2T_q} P_{\text{succ}}^{(L)} P_1 R_2(Q_L), \quad (4.16)$$

with P_1 the sift probability, $R_2(Q) = 1 - 2h_2(Q)$ (or the privacy amplification function appropriate to the protocol), and T_q the time per trial. The recursive bias model yields closed-form expressions for both the QBER and the secret key rate over arbitrary-length paths in the ring. These results explicitly account for bias accumulation and multiplicative heralding across sub-segments, enabling efficient evaluation of end-to-end performance for any selected pair of nodes.

Topology of square-grid quantum networks: A square-grid quantum network extends the repeater chain into two dimensions and 'MANHATTAN' paths, where nodes are arranged in a lattice and connected both horizontally and vertically. Unlike the linear chain, there are multiple parallel paths between pairs of nodes, offering alternative routes, improved redundancy, and potentially lower effective QBER in optimal routing strategies[92].

For the (n,n) square-grid quantum networks, the positions of Bob's and Alice's nodes are set as (x_B, y_B) and (x_A, y_A) , therefore the length of the path $L = (x_B - x_A) + (y_B - y_A)$. For the path selected between $(0,0)$ and $(3,2)$, the path length is $L_0 = L - 1 = 4$. Using the multiplicative bias representation $a_1 \equiv 1 - 2Q_1$ and the repeater noise prefactor k , the end-to-end bias after concatenating six elementary links is obtained by repeated application of the connection rule: $1 - 2Q_2 = k^2 (1 - 2Q_1)^4$. Hence, the sifted QBER on this path reads

$$Q_2 = \frac{1}{2} [1 - k^2 (1 - 2Q_1)^4]. \quad (4.17)$$

The end-to-end heralding (success) probability for the path is the product of elementary-link heralds and internal BSM heralds: $P_{\text{succ}}^{(2)} = P_s(1)^4 P_s^2$. Therefore, the achievable secret key rate for the $(0,0) \rightarrow (3,2)$ path is given as:

$$R_4 = \frac{1}{2T_q} P_{\text{succ}}^{(4)} P_1 R_2(Q_4). \quad (4.18)$$

The example path illustrates how routing over multiple pairs and BSMs affects both bias degradation and end-to-end heralding, providing a baseline for performance comparison across routing strategies.

5 Discussion

5.1 Future Modelling Methods Improvements (HZ, ZX, CM, JS, JMa)

5.1.1 Link Modelling (JS)

The Time-Domain: As highlighted in Section 3.2.1, the simulator could be expanded to support the simulation of the time-domain. This would enable modelling of source emission timing, photon temporal broadening from dispersion, and detector jitter. These factors could be investigated to characterize their effect on network operation synchronisation, such as coincidence counting, interference operations at BSMs, and entanglement swapping.

Unique ITU Channels: The simulator only supports the modelling of M identical ITU channels. As demonstrated in Section 4.6.3, this abstraction becomes unrealistic when channel wavelengths have unequal attenuation rates. The discussed results utilize channels with approximately equal attenuation rates within the L, C, and S-bands, but for increased accuracy and wavelength flexibility, it would be useful to support the simulation of unique parameters for each ITU channel.

5.1.2 Repeater Architecture(ZX, CM)

BSM: As shown in Section 3.3.3, the success rate of BSM is always less than 50%, which greatly limits the key rate. This is because the optical BSM scheme can only distinguish two of the four Bell states. Therefore, another BSM scheme is used in [94]. Based on Rydberg atom processors, the deterministic BSM scheme represents a paradigmatic shift. By leveraging the high-fidelity logical operation capabilities of atomic quantum processors, it transforms BSM from a probabilistic optical process into a deterministic quantum computational process. This not only significantly enhances the operational rate, but more importantly, it seamlessly integrates the core operations of quantum repeaters into scalable, fault-tolerant quantum computing architectures.

QM: To improve the accuracy of communication and entanglement rate calculations in the simulator, the bandwidth and multimode capacity of different quantum memories can be incorporated. Additional models such as NLAMs or emissive memories could also be implemented. For instance, NLAMs offer near-deterministic atom–atom or photon–atom entanglement, improving network success probabilities [28]. Such enhancements, however, come with increased system complexity and integration challenges. Finally, as noted in Section 3.9, modelling qubit behaviour beyond the maximum idle time could be improved by implementing decay rates into the calculation. This would better reflect the characteristics of specific platforms.

5.1.3 QKD Modelling (HZ)

Single Link and Repeater Chains: In future research, the single link and repeater chain models should be refined to address current limitations. For the single link, more realistic channel models are expected to be incorporated, in which time-varying attenuation, polarization drift, and phase noise are included, as they are often observed in deployed quantum channels. Detector performance should be characterized by temperature-dependent noise profiles and variable dark count rates. For the repeater chain, the recursive QBER formulation should be extended to include imperfect entanglement purification, finite quantum memory lifetimes, and stochastic entanglement-swapping success probabilities. Adaptive optimization of the number of elementary links N in response to measured channel conditions should also be considered. By integrating these refinements into a quantum network simulation framework, large-scale performance evaluation can be performed, allowing theoretical limits to be compared against realistic operational scenarios.

Mesh quantum network topology: Future work on ring and square-grid topologies should be directed to incorporating dynamic and fault-tolerant routing. In the ring topology, the effects of variable traffic loads, potential link failures, and routing mechanisms should be systematically evaluated to assess their impact on QKD performance. In the lattice topology, multi-path entanglement distribution and path optimization are to be investigated to take advantage of network redundancy. For both topologies, heterogeneous link qualities, probabilistic link availability, and adaptive path selection algorithms should be integrated into the models. By simulating these structures under realistic noise and loss conditions, their scalability and robustness for deployment in practical quantum networks can be better understood.

5.1.4 Entanglement Purification and Quantum Error Correction (JMa)

Quantum Error Correction (QEC) Under fixed resource budgets (e.g., limited physical qubits, memory positions, and channel uses per logical link), we focus on code families that permit flexible tuning of block length and structure. Generalized quantum parity codes (GQPC) are suitable because their parameters can be adjusted so that, for a given resource envelope and operating regime (set by η_{tr} , detector performance, and quantum-memory noise), the encoding operates near the best achievable point. For the transmission link, we will formulate a constrained design problem that selects the optimal GQPC (block length, redundancy, structure) at each resource level to maximize delivered entanglement fidelity F_{ent} (or throughput) under rate and latency constraints. For quantum memories (QM), given a hardware noise model and device efficiencies (e.g., η_{load} , $\eta_{retrieve}$ contributing to η_m), we will determine the optimal QEC cycle time τ that jointly maximizes effective storage efficiency and achievable storage duration. In practice, the encoder parameters and τ will be co-optimized so that logical performance remains near-optimal without exceeding the available resources specified in Sec. 3.6 and 4.4

Entanglement Purification (EP) In the simulator, the multi-copy nested protocol is used as the default because, under comparable resources, it generally achieves higher final F_{ent} than multi-round DEJMPS. Hyperentanglement-based schemes are not implemented at present, as the current architecture does not provide the hardware to generate and process simultaneous polarization–frequency entanglement at repeater nodes. At present, users choose the purification strategy by inspecting the comparative plots in Sec. 4.8.2 and selecting the method that best matches node conditions and performance targets. Building on this workflow, we will add an automatic EP-selection module that ingests device parameters and priorities (e.g., η_d , η_m , available pairs, WDM channel count M , target F_{ent}) and outputs the protocol and scheduling policy that meet the constraints. Recent results on purification scheduling and protocol choice can be adapted directly to this module [95], [96]. Together with the QEC plan above, EP depth and the GQPC/ τ settings will be co-optimized under the same resource budget to improve end-to-end F_{ent} and effective storage time without exceeding practical limits.

5.2 Future Work

5.2.1 Comparison of Swapping with WDM vs. Ancillary Qubits (JS)

Recent work on Bell-state measurement schemes has explored using ancillary qubits to increase the maximum success probability beyond $\frac{1}{2}$ by simultaneously interfering more than two qubits. This differs from this works method of increasing swapping success probability by attempting M Bell-state measurement between two qubits across M ITU channels and measurement devices. While ancillary qubits can achieve a success probability as high as $\frac{3}{4}$, the effect of stricter synchronisation requirements should be characterised [97].

5.2.2 Comparison of ITU Channel Spacing vs. Source Repetition Rate (JS)

When implementing smaller ITU channel spacings, such as the 0.1 nm channels suggested in Section 4.6.3, this requires utilizing narrower optical filters thereby shortening the coherence length of the transmitted photons. This requires decreasing the source repetition rate to prevent temporal overlap between pulses. Future studies can utilize QUANTA to optimise channel numbers and source repetition rates within the dispersion constraints of the system [5], [82].

5.2.3 Entangled Network Routing (JS, ZX, HZ)

Future work can investigate the effect of trusted vs. untrusted nodes on end-to-end routing schemes across elementary links. Das [98] discuss a mesh network of untrusted nodes utilizing a circuit-switched-like approach, where an end-to-end swapping route is pre-computed based on available elementary links. The performance of this protocol can be compared to a network of trusted nodes, where nodes can dynamically select the best elementary link for swapping at each hop [19], [26]. In addition, Amer [99] further emphasizes that hybrid strategies, where some nodes are trusted while others are untrusted, could offer a balance between performance and security, and merit deeper exploration in future routing protocols.

5.2.4 Alternative and Hybrid Quantum Memory Architectures (CM)

In the future, additional applications of quantum memories in networks can be explored. A key direction is simulating Duan–Lukin–Cirac–Zoller (DLCZ) protocols using emissive quantum memories, where the memories themselves generate herald photons for entanglement creation and Bell-state measurements during swapping. This removes the need for external entanglement sources at each node, though photonic transmission to a central station and classical heralding remain necessary [28]. Another direction is the simulation and characterisation of hybrid quantum-memory protocols that combine complementary strengths, such as Raman–GEM, which couples Raman’s broad bandwidth with GEM’s rephasing control [100].

5.2.5 Further GUI integration (JMc)

Due to time constraints, it wasn't possible to include all the simulations that were conducted in the GUI program. Given more time, implementation of these simulations would be one of the next steps. Originally, we planned to feature a "drag and drop" mode in the simulator where the user could design their own network and run simulations. This presented many complexities that couldn't be overcome in the time frame provided. It requires generalisation of quantum networks to a point where any network could be simulated based just on a few parameters. This would be one of the first next steps in the GUI development.

5.3 Conclusions (All)

Quantum Network Performance with Realistic Hardware Devices: The single link and repeater chain results provided in Section 4 demonstrate the idealistic model provided by Guha [1] overestimates entanglement distribution performance by omitting the simulation of multi-pair emission and detection. The results indicate realistic links detecting multi-pair events achieve the highest fidelity using PNR detectors, which can filter noisy multi-pair detection events. Source-at-Sender link architecture proved to be optimal for high to moderate transmission, while Midpoint-Source links maximized performance at low transmission by dividing the link into two equal fibres to reduce total attenuation. Repeater chains were then simulated with Source-at-Sender links, whose analysis indicated that realistic hardware requires a minimum number of ITU channels to improve the rate of entanglement distribution as more elementary links are added. Inspired by the network architectures of Das [98], repeater chains are networked to simulate a five node network of elementary links. A potential ITU channel allocation scheme is provided to estimate the rates of virtual connection establishment when all users simultaneously request distribution.

Quantum Network Performance with Different Swapping Schemes: The repeater chain results provided in Section 4.2 demonstrate the impact of entanglement swapping protocols on raw key rates, extending Guha's [1] analysis to differentiate sequential, parallel, and binary tree schemes. The full-memory binary tree protocol exhibits superior scalability with logarithmic time complexity, maintaining effective rates for large networks ($N=64$) even at low transmission efficiencies ($\eta_{tr} = 0.01$). The parallel scheme performs optimally only in small networks ($N \leq 4$) with high $\eta_{tr} = 0.9$, but degrades exponentially for $N \geq 16$ due to simultaneous success requirements. The sequential protocol offers balanced performance with linear decay, suitable for medium-scale networks ($N=8-16$) owing to low control complexity. Further comparison of Guha's hybrid binary tree (memoryless first layer with WDM) against full-memory reveals a critical channel threshold $M^* \leq 7$, increasing with link distance(0-100KM), where Guha outperforms by reducing memory needs. Under typical CWDM capabilities (8-32 channels), Guha provides a cost-effective alternative for moderate-loss regimes.

Selectable, Noise-Aware Entanglement Purification and QEC for QKD: The entanglement purification (EP) module's modular architecture offers multiple user-selectable purification schemes and a comprehensive performance comparison framework with multi-dimensional metrics, enabling rigorous cross-protocol evaluation, and explicitly accounting for measurement noise effects within the protocols. Meanwhile, distinct quantum error correction (QEC) strategies – a loss-tolerant parity code for channel photon loss and a five-qubit code for memory decoherence – were tailored to proactively mitigate errors at their source, preserving entanglement integrity in long-distance QKD Seamlessly integrated into the QUANTA simulation platform (encompassing repeater chains with probabilistic entangled photon sources and realistic memory models), these EP and QEC modules collectively bolster the system's robustness and scalability, enabling more reliable and extensible quantum key distribution networks.

GUI Performance: By testing the GUI with students and receiving positive feedback regarding its usability and data visualisation, it's reasonable to conclude that the design of the GUI was a success. However, there is still room for improvement. While the GUI is easy to use and understand, it could be more interesting to look at from a graphic design point of view. This however is a secondary goal and achieving it did not have priority over the functionality and ease of use. Additionally, the program was very responsive and the simulation code ran well at a usable speed for student investigations.

References

- [1] S. Guha, H. Krovi, C. A. Fuchs, *et al.*, Rate-loss analysis of an efficient quantum repeater architecture, *Physical Review A* 2015, 2015.
- [2] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* 2018, 2018.
- [3] H. Takesue and K. Shimizu, Effects of multiple pairs on visibility measurements of entangled photons generated by spontaneous parametric processes, *Optics Communications* 2010, 2010.
- [4] Clark, “Quantum networking through polarisation entanglement distribution,” Ph.D. dissertation, University of Bristol, 2024.
- [5] R. Paschotta, *Coherence time*. available from: www.rp-photonics.com/coherence_time.html.
- [6] D. Chatterjee, “A theoretical investigation of fiber phase sensitive amplifiers for applications,” Ph.D. dissertation, Université Paris-Saclay, 2021.
- [7] J. C. Chapman, J. M. Lukens, M. Alshowkan, N. Rao, B. T. Kirby, and N. A. Peters, Coexistent quantum channel characterization using spectrally resolved bayesian quantum process tomography, *Physical Review Applied* 2023, 2023.
- [8] J. M. Thomas, G. S. Kanter, and P. Kumar, Designing noise-robust quantum networks coexisting in the classical fiber infrastructure, *Optics Express* 2023, 2023.
- [9] J. M. Thomas, F. I. Yeh, J. H. Chen, *et al.*, Quantum teleportation coexisting with classical communications in optical fiber, *Optica* 2024, 2024.
- [10] M. Ghaderibaneh, C. Zhan, H. Gupta, and C. R. Ramakrishnan, Efficient quantum network communication using optimized entanglement swapping trees, *IEEE Transactions on Quantum Engineering* 2022, 2022.
- [11] F. F. Optics, *Dispersion in single mode fiber*. available from: www.fiberoptics4sale.com/blogs/wave-optics/dispersion-in-single-mode-fibers?srsltid=AfmB0orMayXrRtbN7dHYffV2HURmSuQQan5mTSEJ1g-GuaEdExFkhyaK.
- [12] M. Singh, A. K. Sharma, and R. Kaler, Investigations on optical timing jitter in dispersion managed higher order soliton system, *Journal of Optics* 2011, 2011.
- [13] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Invited review article: Single-photon sources and detectors, *Review of scientific instruments* 2011, 2011.
- [14] P. Spot, *Photon spot detector datasheet 2025*. available from: www.photonspot.com/detectors.
- [15] J. Kim, J. Park, H.-S. Kim, *et al.*, Fully controllable time-bin entangled states distributed over 100-km single-mode fibers, *EPJ Quantum Technology* 2024, 2024.
- [16] M. Clementi, F. A. Sabattoli, M. Borghi, *et al.*, Programmable frequency-bin quantum states in a nano-engineered silicon device, *Nature Communications* 2023, 2023.
- [17] S. K. Joshi, D. Aktas, S. Wengerowsky, *et al.*, A trusted node-free eight-user metropolitan quantum communication network, *Science advances* 2020, 2020.
- [18] A. Pljonkin and P. K. Singh, “The review of the commercial quantum key distribution system,” in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, IEEE, 2018.
- [19] P.-Y. Kong, Challenges of routing in quantum key distribution networks with trusted nodes for key relaying, *IEEE Communications Magazine* 2023, 2023.
- [20] A. Farahbakhsh and C. Feng, “Opportunistic routing in quantum networks,” in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, 2022.
- [21] K. Chakraborty, D. Elkouss, B. Rijssman, and S. Wehner, Entanglement distribution in a quantum network: A multicommodity flow-based approach, *IEEE Transactions on Quantum Engineering* 2020, 2020.
- [22] J. Li, Q. Jia, K. Xue, D. S. L. Wei, and N. Yu, A connection-oriented entanglement distribution design in quantum networks, *IEEE Transactions on Quantum Engineering* 2022, 2022.
- [23] L. Kamin, E. Shchukin, F. Schmidt, and P. van Loock, Exact rate analysis for quantum repeaters with imperfect memories and entanglement swapping as soon as possible 2023, 2023.
- [24] M. Peev, C. Pacher, R. Alléaume, *et al.*, The secoqc quantum key distribution network in vienna, *New journal of physics* 2009, 2009.
- [25] P.-Y. Kong, Secret key rate over multiple relays in quantum key distribution for cyber–physical systems, *IEEE Transactions on Industrial Informatics* 2024, 2024.
- [26] A. Abane, M. Cubeddu, V. S. Mai, and A. Battou, Entanglement routing in quantum networks: A comprehensive survey, *IEEE Transactions on Quantum Engineering* 2025, 2025.
- [27] K. Heshami, D. G. England, P. C. Humphreys, *et al.*, Quantum memories: Emerging applications and recent advances, *Journal of Modern Optics* 2016, 2016.
- [28] Y. Lei, F. K. Asadi, T. Zhong, A. Kuzmich, C. Simon, and M. Hosseini, *Quantum optical memory for entanglement distribution*, 2023, arXiv: 2304.09397.
- [29] M. Ivezic, *Quantum memories in quantum networking and computing*, <https://postquantum.com/quantum-networks/quantum-memories/>, 2023.
- [30] A. V. Gorshkov, A. André, M. D. Lukin, and A. S. Sørensen, Photon storage in lambda-type optically dense atomic media. i. cavity model, *Physical Review A* 2007, 2007.
- [31] J. Nunn, K. Reim, K. C. Lee, *et al.*, Multimode memories in atomic ensembles, *Physical Review Letters* 2008, 2008.
- [32] M. P. Hedges, J. J. Longdell, Y. Li, and M. J. Sellars, Efficient quantum memory for light, *Nature* 2010, 2010.
- [33] M. Afzelius, C. Simon, H. de Riedmatten, and N. Gisin, Multimode quantum memory based on atomic frequency combs, *Phys. Rev. A* 2009, 2009.

- [34] M. Gündoğan, P. M. Ledingham, K. Kutluer, M. Mazzera, and H. de Riedmatten, Solid state spin-wave quantum memory for time-bin qubits, *Physical Review Letters* 2015, 2015.
- [35] J. Guo, X. Feng, P. Yang, *et al.*, High-performance raman quantum memory with optimal control in room temperature atoms, *Nature Communications* 2019, 2019.
- [36] B. Albrecht, P. Farrera, X. Fernandez-Gonzalvo, M. Cristiani, and H. de Riedmatten, A waveguide frequency converter connecting rubidium-based quantum memories to the telecom c-band, *Nature Communications* 2014, 2014.
- [37] N. Maring, D. Lago-Rivera, A. Lenhard, G. Heinze, and H. de Riedmatten, Quantum frequency conversion of memory-compatible single photons from 606 nm to the telecom c-band, *Optica* 2018, 2018.
- [38] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication, *Phys. Rev. Lett.* 1998, 1998.
- [39] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, *Reviews of Modern Physics* [online], vol. 83, no. 1 2011, pp. 33–80, 2011. DOI: 10.1103/RevModPhys.83.33.
- [40] S. Muralidharan, C.-L. Zou, L. Li, and L. Jiang, One-way quantum repeaters with quantum reed-solomon codes, *Phys. Rev. A* 2018, 2018.
- [41] K. Azuma, S. E. Economou, D. Elkouss, *et al.*, Quantum repeaters: From quantum networks to the quantum internet, *Reviews of Modern Physics* [online], vol. 95, no. 4 2023, p. 045006, 2023. DOI: 10.1103/RevModPhys.95.045006.
- [42] P. W. Shor, Scheme for reducing decoherence in quantum computer memory 1995, 1995.
- [43] A. M. Steane, Error correcting codes in quantum theory, *Phys. Rev. Lett.* 1996, 1996.
- [44] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, Surface codes: Towards practical large-scale quantum computation 2012, 2012.
- [45] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, Quantum communication without the necessity of quantum memories, *Nature Photonics* 2012, 2012.
- [46] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of noisy entanglement and faithful teleportation via noisy channels, *Physical Review Letters* 1996, 1996.
- [47] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum privacy amplification and the security of quantum cryptography over noisy channels, *Physical Review Letters* 1996, 1996.
- [48] J. Calsamiglia and N. Lütkenhaus, Maximum efficiency of a linear-optical bell-state analyzer, *Applied Physics B* [online], vol. 72, no. 1 2001, pp. 67–71, 2001. DOI: 10.1007/s003400000484.
- [49] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, *Science* 2018, 2018.
- [50] Qt framework, <https://www.qt.io/>, Accessed: 2025-06-01.
- [51] C. Mavelous, J. Ma, J. McDougall, J. Smith, Z. Xu, and H. Zhang, Quanta, <https://github.com/JimbobJames747/CapstoneProj2025.git>, 2025.
- [52] J. D. Hunter, Matplotlib: A 2d graphics environment, *Computing in Science & Engineering* [online], vol. 9, no. 3 2007, pp. 90–95, 2007. DOI: 10.1109/MCSE.2007.55.
- [53] H. K. Beukers, M. Pasini, H. Choi, D. Englund, R. Hanson, and J. Borregaard, Remote-entanglement protocols for stationary qubits with photonic interfaces, *PRX Quantum* 2024, 2024.
- [54] R. Paschotta, Gaussian pulses. available from: www.rp-photonics.com/gaussian_pulses.html.
- [55] OptCore, Dwdm wavelength itu channels chart. available from: www.optcore.net/article057/#FAQs-about-DWDM-Wavelength-Channels.
- [56] V. Balaji, A. Sivasubramanian, E. h. Shaik, *et al.*, 12.5 ghz spectral linewidth optical dwdm photonic crystal demultiplexer in l band communication window, *Optical and Quantum Electronics* 2024, 2024.
- [57] K. Kilinçarslan and S. E. Karlık, Combined impact of srs, fwm and ase noise in udwdm/dwdm long-haul communication systems using edfas, *Optics & Laser Technology* 2023, 2023.
- [58] J.-S. Xu, X.-Y. Xu, C.-F. Li, C.-J. Zhang, X.-B. Zou, and G.-C. Guo, Experimental investigation of classical and quantum correlations under decoherence, *Nature communications* 2010, 2010.
- [59] M. J. Bayerbach, S. E. D'Aurelio, P. Van Loock, and S. Barz, Bell-state measurement exceeding 50% success probability with linear optics, *Science Advances* 2023, 2023.
- [60] L. Zhou and Y.-B. Sheng, Feasible logic bell-state analysis with linear optics, *Scientific Reports* 2016, 2016.
- [61] A. V. Gorshkov, A. André, M. D. Lukin, and A. S. Sørensen, Photon storage in lambda-type optically dense atomic media. ii. free-space model, *Physical Review A* 2007, 2007.
- [62] T.-H. Yang, C.-N. Zhang, J.-P. Dou, *et al.*, Time-bin entanglement built in room-temperature quantum memory, *Phys. Rev. A* 2021, 2021.
- [63] F. Ewert, M. Bergmann, and P. van Loock, Ultrafast long-distance quantum communication with static linear optics, *Phys. Rev. Lett.* 2016, 2016.
- [64] A. Romanova and P. van Loock, Memory-corrected quantum repeaters with adaptive syndrome identification, *Phys. Rev. Res.* 2025, 2025.
- [65] Y.-J. Wang, Z.-Y. Xiao, X.-Y. Xiong, S. Shi, and D.-S. Wang, Generalized quantum parity codes for ultrafast long-distance quantum communication, *Phys. Rev. A* 2025, 2025.
- [66] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, *Phys. Rev. A* 1996, 1996.
- [67] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Perfect quantum error correcting code, *Phys. Rev. Lett.* 1996, 1996.

- [68] J. Kim, J. Yun, and J. Bae, Purification of noisy measurements and faithful distillation of entanglement, *Journal of Physics A: Mathematical and Theoretical* 2024, 2024.
- [69] W. Dür and H. J. Briegel, Entanglement purification and quantum error correction, *Reports on Progress in Physics* 2007, 2007.
- [70] S. Cheng and N. Rengaswamy, *Adaptive error correction for entanglement distillation*, 2025. arXiv: 2504.11670.
- [71] J. Germain, R. Dantu, M. Thompson, and M. Dockendorf, “Quantum networks: Reset-and-reuse can be a game-changer for entanglement via distillation,” in *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, 2022.
- [72] L. Zhou, S.-S. Zhang, W. Zhong, and Y.-B. Sheng, Multi-copy nested entanglement purification for quantum repeaters, *Annals of Physics* 2020, 2020.
- [73] D. Xu, C. Chen, B. T. Kirby, and L. Qian, Entanglement distillation based on polarization and frequency hyperentanglement, *IEEE Journal of Selected Topics in Quantum Electronics* 2024, 2024.
- [74] T. van Leent, M. Bock, R. Garthoff, *et al.*, Long-distance distribution of atom-photon entanglement at telecom wavelength, *Phys. Rev. Lett.* 2020, 2020.
- [75] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, *Physical Review A* 2013, 2013.
- [76] K. Wei, W. Li, H. Tan, *et al.*, High-speed measurement-device-independent quantum key distribution with integrated silicon photonics, *Physical Review X* 2020, 2020.
- [77] Z.-Y. J. Ou, *Quantum Optics for Experimentalists*. World Scientific, 2017.
- [78] L. Ma, X. Lei, J. Yan, *et al.*, High-performance cavity-enhanced quantum memory with warm atomic cell, *Nature Communications*, vol. 13 2022, 2022.
- [79] J. Illiano, M. Caleffi, A. Manzalini, and A. S. Cacciapuoti, Quantum internet protocol stack: A comprehensive survey, *Computer Networks* 2022, 2022.
- [80] T. Coopmans, R. Knegjens, A. Dahlberg, *et al.*, Netsquid, a network simulator for quantum information using discrete events, *Communications Physics* 2021, 2021.
- [81] X. Wu, A. Kolar, J. Chung, *et al.*, Sequence: A customizable discrete-event simulator of quantum networks, *Quantum Science and Technology* 2021, 2021.
- [82] NuCrypt, *Nucrypt eps-1000-w device datasheet*. available from: www.nucrypt.net/EPS-1000-W.html.
- [83] D. E. Mohsen, A. M. Hammadi, and A. J. Al-Askary, Wdm and dwdm based rof system in fiber optic communication systems: A review, *International Journal of Communication Networks and Information Security* 2021, 2021.
- [84] A. K. Ekert, Quantum cryptography based on bell’s theorem, *Phys. Rev. Lett.* 1991, 1991.
- [85] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "event-ready-detectors" bell experiment via entanglement swapping, *Phys. Rev. Lett.* 1993, 1993.
- [86] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, *et al.*, Entanglement-based quantum communication over 144 km, *Nat. Phys.* 2007, 2007.
- [87] X. Liu, X. Yao, R. Xue, *et al.*, A high dimensional entanglement-based fully connected quantum key distribution network, 2019. arXiv: 1910.13743.
- [88] P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, *Physical Review Letters* 2000, 2000.
- [89] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 2005, 2005.
- [90] S. Perseguers, M. Lewenstein, A. Acín, and J. I. Cirac, Quantum random networks, *Nature Physics* 2010, 2010.
- [91] W. Zhang, F. Li, R. Kumar, M. Chen, and L. Zhao, Optimal entanglement distribution within a multi-ring topology, *Scientific Reports* 2025, 2025.
- [92] M. Pant, H. Krovi, D. Towsley, *et al.*, Routing entanglement in the quantum internet, *npj Quantum Information* 2019, 2019.
- [93] A. Acín, J. I. Cirac, and M. Lewenstein, Entanglement percolation in quantum networks, *Nature Physics* 2007, 2007.
- [94] Y.-L. Zhang, Q.-X. Jie, M. Li, *et al.*, Architecture for a quantum repeater based on rydberg-atom quantum processors, *Phys. Rev. Appl.* 2025, 2025.
- [95] L. Chen and Z. Jia, On optimum entanglement purification scheduling in quantum networks, *IEEE Journal on Selected Areas in Communications* [online], vol. 42, no. 7 2024, pp. 1779–1792, 2024. DOI: 10.1109/JSAC.2024.3380080.
- [96] Y. Shi, C. Liu, S. Stein, M. Wang, M. Zheng, and A. Li, *Design of an entanglement purification protocol selection module*, 2024. arXiv: 2405.02555.
- [97] S. Wein, K. Heshami, C. A. Fuchs, *et al.*, Efficiency of an enhanced linear optical bell-state measurement scheme with realistic imperfections, *Physical Review A* 2016, 2016.
- [98] S. Das, S. Khatri, and J. P. Dowling, Robust quantum network architectures and topologies for entanglement distribution 2018, 2018.
- [99] O. Amer, W. O. Krawec, M. Z. Hossain, V. U. Manfredi, and B. Wang, “Dynamic routing and post-processing strategies for hybrid quantum key distribution networks,” in *2024 IEEE 44th International Conference on Distributed Computing Systems (ICDCS)*, 2024.
- [100] G. Hétet, M. Hosseini, B. M. Sparkes, D. Oblak, P. K. Lam, and B. C. Buchler, Photon echoes generated by reversing magnetic field gradients in a rubidium vapor, *Opt. Lett.* 2008, 2008.