ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

INTERNATIONAL HELLENIC UNIVERSITY
DEPARTMENT OF INFORMATION AND ELECTRONIC ENGINEERING

THESIS

«Quantum Communication Algorithms via Satellite Link»

Student:
Charilaos Christos Angelidis
Student ID:2021002

Supervisor
Ioannis K. Marmorkos
Professor

January 21, 2026

Title of Dissertation Quantum Communication Algorithms via Satellite Link
Code of Dissertation 25354
Student's full name Charilaos Christos Angelidis
Supervisor's full name Ioannis K. Marmorkos
Date of undertaking 12-11-2025
Date of completion 02-01-2026

I hereby affirm the authorship of this paper as well as the acknowledgement and credit of whichever assistance I received in its composition. I have, furthermore, noted the various sources from which I extracted data, ideas, visual or written material, in paraphrase or exact quotation. Moreover, I affirm the exclusive composition of this paper by myself only, for the purpose of it being a dissertation, in the Department of Information and Electrical Engineering of the International Hellenic University.

The approval of this dissertation by the Department of Information and Electronic Engineering of the International Hellenic University, does not necessarily entail the adoption of the author's views, on behalf of the Department.

To my family

Prolog

Quantum computing is a field that emerged in the 1980s and has since experienced remarkable progress.

Quantum algorithms and communication protocols, which exploit the fundamental principles of quantum mechanics to enhance performance, demonstrate that quantum computing represents the future of information science and communications.

From the very first lecture of the course Quantum Computing, I felt a deep and genuine enthusiasm for this new world that was unfolding before me. This thesis has helped me gain a deeper understanding of the foundations of quantum computing and allowed me to explore a number of highly intriguing topics. I hope that it may also inspire and assist others in discovering, or further exploring, this fascinating field of quantum computing.

Abstract

En

Quantum communication promises fundamentally secure information exchange by exploiting the principles of quantum mechanics, such as superposition, entanglement, and the no-cloning theorem. In recent years, satellite-based quantum communication has emerged as a key enabling technology for extending quantum networks to global scales, overcoming the distance limitations imposed by optical fibers. This thesis provides a comprehensive study of quantum communication protocols and their physical implementation through satellite links, with particular emphasis on uplink-based architectures.

The first part of the thesis introduces the theoretical foundations of quantum information, including quantum states, quantum gates, entanglement, and representative quantum algorithms and key distribution protocols. Subsequently, established quantum key distribution schemes and entanglement-based protocols are reviewed, highlighting their security principles and practical constraints.

The core contribution of this work lies in the detailed analysis of satellite-assisted quantum communication architectures. A well-established double-uplink entanglement swapping configuration is first examined using realistic physical models that account for diffraction, atmospheric turbulence, background noise, and detection inefficiencies. Building upon this analysis, the thesis extends the modeling framework to underexplored dual-satellite dual uplink and hybrid uplink-downlink architectures, where entanglement distribution is achieved without intermediate swapping operations.

Numerical simulations demonstrate that hybrid architectures can significantly mitigate the severe loss scaling associated with double-uplink schemes, leading to substantial improvements in entanglement distribution rates under realistic Low Earth Orbit conditions. The results highlight the importance of link asymmetry and identify the uplink as the dominant performance bottleneck.

Overall, this thesis contributes a unified analytical and numerical framework for evaluating satellite-based quantum communication architectures and provides insights into promising design directions for future global quantum networks

Gr

Η κβαντική επικοινωνία υπόσχεται θεμελιωδώς ασφαλή ανταλλαγή πληροφορίας, αξιοποιώντας βασικές αρχές της κβαντομηχανικής, όπως η κβαντική υπέρθεση, η κβαντική σύμπλεξη και το θεώρημα της μη κλωνοποίησης. Τα τελευταία χρόνια, η δορυφορική κβαντική επικοινωνία έχει αναδειχθεί ως τεχνολογία-κλειδί για την επέκταση των κβαντικών δικτύων σε παγκόσμια κλίμακα, ξεπερνώντας τους περιορισμούς απόστασης των οπτικών ινών. Η παρούσα διπλωματική εργασία παρουσιάζει μια ολοκληρωμένη μελέτη κβαντικών επικοινωνιακών πρωτοκόλλων και της φυσικής τους υλοποίησης μέσω δορυφορικών ζεύξεων, με ιδιαίτερη έμφαση στις αρχιτεκτονικές ανόδου (uplink).

Στο πρώτο μέρος παρουσιάζονται τα θεωρητικά θεμέλια της κβαντικής πληροφορίας, συμπεριλαμβανομένων των κβαντικών καταστάσεων, των κβαντικών πυλών, της κβαντικής εμπλοκής, καθώς και αντιπροσωπευτικών κβαντικών αλγορίθμων και πρωτοκόλλων κατανομής κλειδιού. Στη συνέχεια, αναλύονται καθιερωμένα πρωτόκολλα κβαντικής κατανομής κλειδιού και πρωτόκολλα βασισμένα στην εμπλοκή, με έμφαση στις αρχές ασφάλειας και στους πρακτικούς περιορισμούς τους.

Η κύρια συνεισφορά της εργασίας εντοπίζεται στη λεπτομερή ανάλυση δορυφορικά υποβοηθούμενων αρχιτεκτονικών κβαντικής επικοινωνίας. Αρχικά εξετάζεται μια καθιερωμένη αρχιτεκτονική διπλού uplink με entanglement swapping, χρησιμοποιώντας ρεαλιστικά φυσικά μοντέλα που λαμβάνουν υπόψη τη περίθλαση, την ατμοσφαιρική τύρβη, τον θόρυβο υποβάθρου και τις αποδόσεις ανίχνευσης. Βασιζόμενη σε αυτήν την ανάλυση,η εργασία επεκτείνει το πλαίσιο ανάλυσης σε αρχιτεκτονικές uplink δύο δορυφόρων και υβριδικές αρχιτεκτονικές uplink–downlink, οι οποίες παραμένουν ελάχιστα διερευνημένες στη βιβλιογραφία.

Αριθμητικές προσομοιώσεις δείχνουν ότι οι υβριδικές αρχιτεκτονικές μπορούν να μετριάσουν σημαντικά την αυστηρή κλιμάκωση απωλειών των διπλών uplink σχημάτων, οδηγώντας σε ουσιαστική αύξηση των ρυθμών διανομής εμπλοκής υπό ρεαλιστικές συνθήκες χαμηλής γήινης τροχιάς. Τα αποτελέσματα αναδεικνύουν την ασυμμετρία των ζεύξεων και προσδιορίζουν το uplink ως το κυρίαρχο σημείο συμφόρησης του συστήματος.

Συνολικά, η εργασία συνεισφέρει ένα ενιαίο αναλυτικό και αριθμητικό πλαίσιο για την αξιολόγηση δορυφορικών αρχιτεκτονικών κβαντικής επικοινωνίας και προσφέρει κατευθυντήριες γραμμές για τον σχεδιασμό μελλοντικών παγκόσμιων κβαντικών δικτύων.

Thanks

I would like to thank my supervisor Dr. Ioannis K. Marmorkos for his invaluable help throughout the writing of my thesis.

Contents

List of Figures

List of Tables

Abbreviations

QIS	Quantum Information Science
QKD	Quantum Key Distribution
SNR	Signal to Noise Ratio
LEO	Low Earth Orbit
QBER	Quantum Bit Error Rate
CNOT	Controlled NOT
CCNOT	Controlled Controlled NOT
MDI	Measurement Device Independent
BSM	Bell-State Measurement
SDK	Software Developing Kit
FOV	Field Of View
SWaP	Size, Weight and Power
PAA	Point-Ahead Angle
PAT	Point-Ahead Tracking
ISL	Inter-Satellite Link
AO	Adaptive Optics
E2E	End to End

Chapter 1: Introduction

1.1 Historical Context

1.1.1 The Limits of Classical Computation

The latter half of the 20th century was defined by the digital revolution, driven essentially by the invention of the transistor in 1947. For decades, the evolution of computing power followed the empirical observation known as **Moore's Law**. Proposed by Gordon Moore in 1965 [1], this law predicted that the number of transistors on a dense integrated circuit would double approximately every two years, leading to an exponential increase in computational power and a corresponding decrease in cost.

For over fifty years, the semiconductor industry successfully upheld this trend by shrinking the size of transistors. However, as feature sizes began to approach the atomic scale (nanometers), engineers encountered fundamental physical barriers. At such minute scales, classical physics fails to describe the behavior of electrons accurately. Phenomena such as **quantum tunneling**-where electrons probabilistically pass through insulating barriers-cause leakage currents [2, 3] that generate excessive heat and render logic gates unreliable. It became evident that the miniaturization of classical components would eventually hit a hard wall imposed by the laws of thermodynamics and quantum mechanics. This realization prompted the scientific community to explore whether these quantum effects, rather than being a hindrance, could be harnessed for computation.

1.1.2 The Genesis of Quantum Computing

The recognition of the fundamental physical limits of classical computation marked a pivotal turning point in the history of information processing. As classical devices approached regimes where quantum effects could no longer be neglected, a profound question emerged: rather than combating quantum phenomena, could they be exploited as a computational resource? This question laid the conceptual foundation for what is now known as **quantum computing**.

The earliest formal connection between computation and quantum mechanics can be traced back to the work of Richard Feynman in the early 1980s. Feynman observed that simulating quantum systems using classical computers incurs an exponential overhead in resources, as the size of the Hilbert space describing a quantum system grows exponentially with the number of particles. In his seminal 1982 paper [4], he proposed that a machine governed by the laws of quantum mechanics would be inherently more efficient at simulating quantum phenomena than any classical counterpart. This insight suggested a radical shift in computational paradigms: the very features that hinder classical miniaturization-superposition and entanglement-could enable new forms of information processing.

Building on this idea, David Deutsch provided the first rigorous theoretical framework for quantum com-

putation in 1985 by introducing the concept of a **universal quantum computer** [5]. Deutsch generalized the classical Turing machine to the quantum domain, demonstrating that a finite set of quantum gates could approximate any unitary transformation with arbitrary precision. This result established quantum computation as a well-defined computational model, independent of specific physical implementations, and placed it on equal theoretical footing with classical computation.

A defining characteristic of quantum computation is the representation of information using **quantum bits**, or qubits. Unlike classical bits, which exist in one of two definite states, qubits can exist in coherent superpositions of basis states. When multiple qubits are combined, they can form entangled states that exhibit correlations with no classical analogue. These uniquely quantum resources allow quantum computers to process information in ways fundamentally inaccessible to classical machines, enabling parallelism in the state space rather than in explicit computational paths.

1.1.3 The Algorithmic Revolution

While the physical realization of quantum computers is driven by advances in experimental physics and engineering, the true transformative power of quantum computation is revealed at the algorithmic level. The emergence of quantum algorithms that demonstrably outperform their classical counterparts marked a decisive moment in the development of quantum information science. This algorithmic revolution provided concrete evidence that quantum mechanics enables new computational capabilities rather than merely offering an alternative hardware platform.

At the heart of quantum algorithms lies a fundamentally different mode of information processing. Classical algorithms operate on definite bit values and explore computational paths sequentially or through classical parallelism. Quantum algorithms, by contrast, exploit quantum superposition to encode information across an exponentially large state space, while quantum interference is used to amplify correct outcomes and suppress incorrect ones. Importantly, this so-called “quantum parallelism” does not yield direct access to all computed results. Instead, carefully designed interference patterns ensure that the desired solution is obtained with high probability upon measurement.

The first major demonstration of a quantum algorithmic advantage was provided by Peter Shor in 1994 [6]. Shor’s algorithm showed that integer factorization and discrete logarithms-problems believed to be intractable for classical computers-can be solved in polynomial time on a quantum computer. This result had profound implications, as it directly threatened the security of widely deployed cryptographic protocols such as the RSA. Beyond its practical consequences, Shor’s algorithm established that quantum computation can offer an exponential speedup over the best known classical algorithms for certain problems.

Shortly thereafter, Lov Grover introduced a quantum algorithm for unstructured database search that achieves a quadratic speedup compared to classical methods [7]. Although less dramatic than the exponential advantage of Shor’s algorithm, Grover’s algorithm is remarkable for its generality: it applies to any problem that can be framed as a search over an unstructured solution space. This result demonstrated that quantum speedups are not limited to highly specialized problems, but can arise in broad algorithmic contexts.

Taken together, the algorithmic revolution transformed quantum computing from a theoretical curiosity into a compelling computational paradigm. By revealing problems for which quantum mechanics enables provable or conjectured speedups, quantum algorithms clarified the practical and theoretical significance of quantum computation. This shift in perspective continues to guide modern research, motivating the search for new quantum algorithms and deepening our understanding of the interplay between physics and computation.

1.1.4 The Rise of Quantum Information Science

The development of quantum computing and quantum algorithms catalyzed the emergence of a broader and more unifying framework known as **Quantum Information Science** (QIS). Rather than focusing exclusively on computation, QIS studies information as a physical entity governed by the laws of quantum mechanics. This shift in perspective redefined long-standing concepts such as information storage, transmission, and processing, placing them within a fundamentally quantum-mechanical context.

A central insight underlying quantum information science is that information cannot be divorced from the physical systems that encode it. Classical information theory, pioneered by Claude Shannon, treats information abstractly and independently of its physical realization. In contrast, quantum information theory explicitly accounts for the constraints and possibilities imposed by quantum mechanics. Principles such as the **no-cloning theorem**, the **uncertainty principle**, and **quantum measurement back-action** impose fundamental limits on how quantum information can be copied, measured, and transmitted, while simultaneously enabling novel capabilities absent in classical systems.

One of the most striking consequences of this paradigm is the recognition of **quantum entanglement** as a genuine informational resource. Once regarded primarily as a philosophical curiosity, entanglement is now understood to underpin many quantum information protocols, including quantum teleportation, superdense coding, and entanglement-based quantum cryptography. These protocols demonstrate that quantum correlations can enhance communication efficiency and security beyond classical limits, thereby extending the scope of information science into fundamentally new territory.

The rise of quantum information science also fostered a deep synthesis between previously distinct disciplines. Concepts from computer science, such as computational complexity and error correction, were reformulated in the quantum domain, leading to the development of **quantum error correction** and **fault-tolerant computation**. Remarkably, quantum error-correcting codes showed that fragile quantum states could be protected against decoherence and noise without violating the principles of quantum mechanics, addressing a major obstacle to scalable quantum technologies.

In conclusion, the rise of quantum information science represents a unification of physics, computation, and information theory. By treating information as a physical quantity subject to quantum laws, QIS has reshaped both our theoretical understanding and practical exploitation of quantum systems. This interdisciplinary field now forms the backbone of modern quantum technologies, encompassing quantum computing, quantum communication, and quantum sensing within a coherent and rapidly evolving scientific framework.

1.2 Quantum Communication

Quantum communication constitutes one of the most mature and experimentally advanced branches of quantum information science. Its primary objective is the transmission of information encoded in quantum states across spatially separated locations, exploiting the principles of quantum mechanics to achieve functionalities that are impossible within classical communication frameworks. Unlike classical communication, which relies on the transmission of classical bits through electromagnetic signals, quantum communication operates on **quantum states** and is fundamentally constrained and empowered by quantum measurement, superposition, and entanglement.

1.2.1 Foundations of Quantum Communication

At the core of quantum communication lies the concept of a **quantum channel**, which describes the physical process by which quantum states are transmitted from a sender to a receiver. In practical implementations, quantum channels are inherently noisy due to decoherence, photon loss, and environmental interactions, necessitating a rigorous information-theoretic treatment.

A fundamental distinction between classical and quantum communication arises from the impossibility of perfectly copying unknown quantum states, as formalized by the **no-cloning theorem**. This restriction prohibits the use of classical signal amplification techniques and has profound consequences for long-distance communication. At the same time, it provides the basis for intrinsically secure communication protocols, as any eavesdropping attempt inevitably disturbs the transmitted quantum states.

1.2.2 Quantum Key Distribution

The most prominent and technologically mature application of quantum communication is **Quantum Key Distribution** (QKD). QKD protocols enable two distant parties to establish a shared secret key with information-theoretic security guaranteed by the laws of quantum mechanics, rather than by computational hardness assumptions.

Modern QKD systems incorporate advanced techniques including decoy states, error correction, and privacy amplification, enabling secure key exchange over optical fibers and free-space links spanning hundreds of kilometers.

1.2.3 Entanglement-Based Communication and Quantum Teleportation

Entanglement plays a central role in quantum communication beyond cryptography. In entanglement-based protocols, spatially separated parties share entangled quantum states that serve as a resource for communication tasks. A paradigmatic example is **quantum teleportation**, in which an unknown quantum state is transmitted using a combination of shared entanglement and classical communication, without physically sending the quantum system itself.

Quantum teleportation illustrates a profound separation between information and physical carriers. The protocol preserves all quantum properties of the transmitted state, including coherence and entanglement

with other systems, making it indispensable for quantum networks and distributed quantum computing. Closely related protocols, such as superdense coding, demonstrate that entanglement can increase the classical information capacity of a quantum channel beyond classical limits.

1.2.4 Quantum Repeaters and Long-Distance Communication

A major challenge in quantum communication is the exponential attenuation of quantum signals over distance, particularly in optical fibers. Due to the no-cloning theorem, classical repeaters cannot be directly adapted to the quantum domain. This limitation motivated the development of **quantum repeaters**, which enable long-distance communication through entanglement distribution, entanglement swapping, and entanglement purification.

Quantum repeaters divide long communication links into shorter segments, establish entanglement locally, and progressively extend it across the network. Although significant experimental progress has been made, the realization of scalable and efficient quantum repeaters remains an active area of research, requiring advances in quantum memories, error correction, and synchronization.

1.2.5 Quantum Networks and Satellite-Based Implementations

Quantum networks represent an evolutionary stage from point-to-point quantum communication towards the realization of a fully global quantum infrastructure. At this level, the primary objective is the physical distribution of quantum states and entanglement across multiple nodes using available transmission media, such as optical fibers and free-space optical links. These networks serve as experimental testbeds for validating quantum communication protocols under realistic conditions.

Terrestrial quantum networks are predominantly based on optical fiber technology, leveraging mature telecommunication infrastructure. Metropolitan-scale fiber networks have successfully demonstrated quantum key distribution and entanglement distribution across multiple nodes [8–10]. However, photon loss in optical fibers increases exponentially with distance, imposing severe limitations on the maximum achievable separation between network nodes without the use of quantum repeaters [11, 12].

Free-space optical communication provides an alternative approach, particularly suited for long-distance and mobile scenarios. In this context, satellite-based quantum communication has emerged as a promising solution for overcoming the distance limitations of terrestrial networks. Low-Earth-orbit (LEO) satellites enable quantum links between distant ground stations by transmitting single photons or entangled photon pairs through the atmosphere and outer space, where attenuation is significantly reduced compared to optical fibers.

Satellite-based implementations introduce unique technical challenges, including beam divergence, pointing and tracking accuracy, atmospheric turbulence, and background noise. Nevertheless, landmark experiments have demonstrated satellite-to-ground quantum key distribution and long-distance entanglement distribution, confirming the feasibility of intercontinental quantum links. These achievements highlight the crucial role of space-based platforms in extending the reach of quantum communication beyond terrestrial constraints.

Overall, quantum networks and satellite-based implementations establish the physical foundation for large-scale quantum communication. While these systems enable the distribution of quantum states across increasing distances, they primarily focus on the reliable realization of individual quantum links rather than on the global coordination and utilization of entanglement as a network-wide resource.

1.2.6 The Quantum Internet

The quantum internet represents the next conceptual and technological leap beyond individual quantum links and local quantum networks [13,14]. It envisions a global, scalable infrastructure in which quantum information is distributed, processed, and utilized across geographically separated nodes through a fundamentally new networking paradigm. Unlike classical networks, which route and amplify classical data, the quantum internet is built upon the controlled creation, distribution, and utilization of entanglement.

A defining characteristic of the quantum internet is the treatment of entanglement as a fundamental networking resource. Rather than transmitting quantum states directly over long distances, remote nodes establish shared entangled states that enable quantum communication through protocols such as quantum teleportation and entanglement swapping. In this framework, quantum information is effectively transferred by exploting entanglement in conjunction with classical communication, ensuring that quantum coherence is preserved across the network.

The architecture of a quantum internet is inherently hybrid, combining quantum and classical communication layers. The classical layer is responsible for network coordination, synchronization, routing decisions, and the transmission of measurement outcomes, while the quantum layer handles the generation, storage, and distribution of quantum states. This hybrid structure is essential, as most quantum communication protocols fundamentally rely on classical information exchange alongside quantum resources.

Scalability remains one of the central challenges in realizing a functional quantum internet. Photon loss, decoherence, and finite coherence times of quantum memories limit the reliable distribution of entanglement across large distances. To address these challenges, quantum repeaters, entanglement purification, and quantum error correction are indispensable components of quantum internet architectures. Efficient and long-lived quantum memories are particularly critical for enabling asynchronous network operation and large-scale entanglement distribution.

Beyond secure communication, the quantum internet enables applications with no classical analogue. These include distributed quantum computing, where multiple quantum processors collaborate to solve computational tasks, and networked quantum sensing, which exploits entanglement to enhance measurement precision across spatially separated sensors. Furthermore, large-scale quantum networks provide unique platforms for testing fundamental aspects of quantum mechanics, including nonlocality and entanglement over unprecedented distances.

In summary, the quantum internet extends quantum communication from isolated physical links to a global, entanglement-based network architecture. By elevating entanglement to a core networking primitive, it transcends classical communication paradigms and establishes the foundation for future distributed quantum technologies.

1.2.7 Challenges and Outlook

Despite remarkable progress, quantum communication faces significant technical and theoretical challenges. Photon loss, decoherence, limited detector efficiency, and the scalability of quantum memories remain critical bottlenecks. Moreover, the characterization and verification of quantum communication channels often require sophisticated techniques such as quantum state and process tomography.

Nevertheless, continued advances in photonics, materials science, and quantum information theory are rapidly closing the gap between theoretical protocols and real-world implementations. As a cornerstone of quantum information science, quantum communication is expected to play a pivotal role in the development of future quantum technologies, enabling secure communication, distributed quantum computation, and large-scale quantum networks.

1.3 Thesis Outline

This thesis is organized into seven chapters, structured as follows:

Chapter 1: Introduction
This chapter provides the historical context and motivation for the study of quantum information science. It outlines the limitations of classical computing that led to the development of the quantum paradigm and defines the scope and objectives of this thesis.

Chapter 2: Quantum Computing
This chapter establishes the theoretical framework of quantum mechanics required for computation. We introduce the concept of the qubit, the Bloch sphere representation, and quantum gates. Furthermore, we present a detailed analysis of fundamental quantum algorithms, including Deutsch's, Simon's, and Shor's algorithms.

Chapter 3: Protocols and Algorithms for Quantum Communications
This chapter focuses on the protocols governing the transmission of quantum information. We analyze the No-Cloning Theorem and its implications for security. Key protocols are examined, including Quantum Key Distribution, Quantum Teleportation, and Entanglement Swapping.

Chapter 4: Qiskit and IBM Quantum Composer: A Practical Introduction
We introduce the software ecosystem used for quantum experimentation. This chapter presents Qiskit, the open-source SDK for programmatic circuit control, alongside the IBM Quantum Composer, a graphical interface for intuitive circuit design. Together, these tools provide the technical foundation for the simulations and hardware executions presented later in this work.

Chapter 5: Satellite Link Elements
This chapter analyzes the fundamental components and characteristics of satellite communication links. We discuss orbital mechanics, free-space optical channel modeling, atmospheric turbulence, and attenuation factors that critically affect the transmission of quantum states between ground stations and satellites.

Chapter 6: Entanglement Distribution via Satellite Link
In this chapter, we integrate the theoretical models with practical simulation. We implement the quantum

communication algorithms discussed in Chapter 3 over the satellite link channel modeled in Chapter 5. We evaluate the performance and feasibility of these protocols under realistic channel conditions.

Chapter 7: Conclusions and Future Work
The final chapter summarizes the key findings of this thesis. We draw conclusions regarding the viability of satellite-based quantum communications and outline potential directions for future research, including error correction techniques and the development of quantum repeater networks.

Chapter 2: Quantum Computing

2.1 Introduction

This chapter provides the reader with the necessary background on quantum computing. It starts with the core elements of quantum mechanics and introduces the qubit. It then presents quantum gates and quantum circuits, concluding with an overview of the fundamental quantum algorithms.

2.2 Elements of Quantum Mechanics

2.2.1 Dirac Notation

A vector is a physical quantity that consists of an ordered tuple of numbers. Vectors can be represented as row or column matrices. The elements of the matrix correspond to the vector components with respect to an orthonormal basis of dimension n. A typical vector $\vec{\mathbf{v}}$ of the three-dimensional {**x,y,z**} basis can be expressed as:

$$\vec{v} = \begin{bmatrix} a \\ b \\ c \end{bmatrix} = a\hat{\boldsymbol{x}} + b\hat{\boldsymbol{y}} + c\hat{\boldsymbol{z}} \tag{2.1}$$

This can be generalized for an n-dimensional space:

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \in \mathbb{R}^n \tag{2.2}$$

Vectors in quantum mechanics follow a specific notation known as Dirac notation (or Bra-Ket notation), introduced by physicist Paul Dirac in 1939 [15]. From now on, a vector $\vec{\mathbf{v}}$ will be expressed using Dirac notation as $|v\rangle$. Vector $|v\rangle$ can be expressed with its complex components $v_i \in \mathbb{C}$ in a canonical basis of space $\mathbb{V}^n$ as:

$$|v\rangle = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \tag{2.3}$$

Vector $|v\rangle$ is pronounced **ket v**. For every n-dimensional vector space $\mathbb{V}^n$, a dual space $\mathbb{V}^{n*}$ can be defined. The vectors of this dual space are derived through a one-to-one mapping from space $\mathbb{V}^n$. These dual vectors, which are called **bras**, represented as $\langle v|$, are expressed as a row matrix. This row matrix

is the conjugate transpose (denoted †) of the column matrix of the equivalent ket:

$$\langle v| = \begin{bmatrix} v_1^*, & v_2^*, & \cdots & , v_n^* \end{bmatrix} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}^\dagger \tag{2.4}$$

2.2.2 Inner Product

The inner product of two vectors $|v\rangle$, $|w\rangle \in \mathbb{V}^n$ is a function of the two vectors, resulting in a complex number and defined as:

$$\langle v|w\rangle = \begin{bmatrix} v_1^*, & v_2^*, & \cdots & , v_n^* \end{bmatrix} \times \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \sum_{i=1}^{n} v_i^* w_i \tag{2.5}$$

The inner product has the following properties:

$$\langle v|w\rangle = \langle w|v\rangle^* \tag{2.6}$$

$$\langle v|\alpha z + \beta w\rangle = \alpha \langle v|z\rangle + \beta \langle v|w\rangle \,,\ \alpha, \beta \in \mathbb{C} \tag{2.7}$$

$$\langle \alpha z + \beta w|v\rangle = \alpha^* \langle z|v\rangle + \beta^* \langle w|v\rangle \,,\ \alpha, \beta \in \mathbb{C} \tag{2.8}$$

Two vectors $|v\rangle$,$|w\rangle \in \mathbb{V}^n$ are said to be **orthogonal** when their inner product is equal to zero:

$$\langle v|w\rangle = 0 \Rightarrow |v\rangle \perp |w\rangle \tag{2.9}$$

Using the inner product, the norm of a vector $|v\rangle$ can be defined as:

$$\||v\rangle\| = \sqrt{\langle v|v\rangle} = \sqrt{\sum_{i=1}^{n} v_i^* v_i} = \sqrt{\sum_{i=1}^{n} |v_i|^2} \tag{2.10}$$

A vector $|v\rangle$ is called a **unit vector**, if its norm is equal to one. From any given vector $|v\rangle$ a unit vector, denoted $|\hat{\boldsymbol{v}}\rangle$ can be constructed. This process is called **normalization** and it is achieved by dividing the vector by its norm:

$$|\hat{\boldsymbol{v}}\rangle = \frac{|v\rangle}{\||v\rangle\|} \tag{2.11}$$

This property plays a central role in quantum computing as every qubit state is represented by a unit vector.

2.2.3 Hilbert Spaces and orthonormal Bases

A Hilbert space is a complete complex vector space equipped with an inner product. It should be noted that in quantum mechanics, a ket that represents the state of a quantum system is a vector in a Hilbert

space.

A vector basis $\{ |v_1\rangle,|v_2\rangle,\ldots,|v_n\rangle\} \in \mathbb{C}^n$ is called **orthonormal** when for every pair of $|v_i\rangle, |v_j\rangle$ the following equation is true:

$$\langle v_i|v_j\rangle = \delta_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \tag{2.12}$$

δ_{ij} is called the **Kronecker delta**. That means that all vectors are unit vectors and orthogonal to each other. Note that most bases used in quantum computing are orthonormal.

2.2.4 Operators

Operators are mathematical entities that act on vectors and transform them. The action of an operator A upon a vector $|v\rangle$ is defined as:

$$A|v\rangle = |w\rangle \tag{2.13}$$

Similarly, operators acting on bras are defined as:

$$B\langle v| = \langle w| \tag{2.14}$$

The sum $C = A + B$ of two operators is defined as:

$$C|v\rangle = (A + B)|v\rangle = A|v\rangle + B|v\rangle \tag{2.15}$$

The product of two operators implies a specific order of application, acting from right to left:

$$AB|v\rangle = A(B|v\rangle) = A|w\rangle \tag{2.16}$$

It follows that the commutative property applies to the sum ($A+B = B+A$) , but not to the product of two operators ($AB \neq BA$).

We can define the **commutator** of two operators A and B as:

$$[A, B] = AB - BA \tag{2.17}$$

In quantum computing the operators that are used are **linear operators**. For an operator A to be linear, the following property must be true:

$$A(\alpha|v\rangle + \beta|w\rangle) = \alpha A|v\rangle + \beta A|w\rangle, \ \alpha, \beta \in \mathbb{C} \tag{2.18}$$

2.2.4.1 The Identity Operator

The identity operator (denoted I) acts upon a vector without transforming it.

$$I|v\rangle = |v\rangle \tag{2.19}$$

The identity operator is represented as a matrix with every element equal to zero, except for the diagonal elements, which are equal to one:

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \tag{2.20}$$

2.2.4.2 Outer Product

The outer product of two vectors $|v\rangle$, $|w\rangle$, denoted $|v\rangle\langle w|$, is defined as a linear operator P, that acts upon a vector $|z\rangle$ as:

$$P\,|z\rangle = |v\rangle\,\langle w|z\rangle = (\langle w|z\rangle)\,|v\rangle \tag{2.21}$$

Recalling that the inner product of two vectors results in a complex number (scalar result), it can be said that the operator

$$P = |v\rangle\,\langle w| \tag{2.22}$$

acting on a ket $|z\rangle$ produces a vector in the direction of $|v\rangle$, scaled by the scalar $\langle w|z\rangle$.

2.2.4.3 Hermitian Operators

Given a ket $|v\rangle$ and an operator A, the act of the operator on the vector is defined as:

$$|w\rangle = |Av\rangle = A\,|v\rangle \tag{2.23}$$

The same applies for the equivalent bra $\langle v|$:

$$\langle w| = \langle Av| = \langle v|\,A^\dagger \tag{2.24}$$

Operator $A^\dagger$ is defined as the operator that transforms $\langle v|$ to $\langle w|$ and is called the **Hermitian conjugate** of operator A. The following properties are true for Hermitian conjugate operators:

$$(A^\dagger)^\dagger = A \tag{2.25}$$

$$\langle v|\,A = \left\langle A^\dagger v\right| \tag{2.26}$$

$$(AB)^\dagger = B^\dagger A^\dagger \tag{2.27}$$

$$(A+B)^\dagger = A^\dagger + B^\dagger \tag{2.28}$$

An operator A is called **Hermitian** if it is equal to its Hermitian conjugate operator

$$A = A^\dagger \tag{2.29}$$

Hermitian operators play a central role in quantum computing as they represent all physical quantities of a quantum system.

2.2.4.4 Unitary Operators

A unitary operator U satisfies the following property:

$$UU^\dagger = U^\dagger U = I \Rightarrow U^\dagger = U^{-1} \tag{2.30}$$

The inner product of two vectors is not affected by the act of a unitary operator on the vectors. If

$$|w_1\rangle = U\,|v_1\rangle \tag{2.31}$$

and

$$|w_2\rangle = U\,|v_2\rangle \tag{2.32}$$

then

$$\langle w_2|w_1\rangle = \langle Uv_2|Uv_1\rangle = \langle v_2|\,U^\dagger U\,|v_1\rangle = \langle v_2|v_1\rangle \tag{2.33}$$

Essentially, a unitary operator acting on a vector preserves the norm of the vector and simply rotates it within the Hilbert space. This property is fundamental in quantum computing, as it ensures that the total probability remains conserved (equal to 1) during the evolution of a closed quantum system.

2.2.4.5 Pauli Operators

The following operators, called Pauli operators [16], are proven to be useful in quantum mechanics.

$$\begin{aligned}
\sigma_0 = I &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
\sigma_1 = \sigma_x = X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\
\sigma_2 = \sigma_y = Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\
\sigma_3 = \sigma_z = Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}
\end{aligned} \tag{2.34}$$

All four Pauli operators are Hermitian and unitary.

2.2.5 Axioms of Quantum Mechanics

In the following section, the fundamental axioms of quantum mechanics [17, 18] are presented.

2.2.5.1 First Axiom: The state of a Quantum System

The state of a quantum system is represented by a unit vector of a Hilbert vector space. This vector, called the **state vector** contains all information about the system. The dimension of the equivalent Hilbert space can be either infinite or finite. In quantum computing most systems are two-dimensional, also called **two-level systems**. The basic unit of a quantum computer, the qubit, is a two-level system. The basis of such a system is composed of two linearly independent and orthogonal unit vectors. The most frequently used computational basis consists of ket $|0\rangle$ and ket $|1\rangle$. The basis $\{\ |0\rangle, |1\rangle\ \} \in \mathcal{H}^2$ is also called **canonical basis**. The generalized state of a two-level system using the canonical basis is represented by state vector $|\psi\rangle$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix},\ \alpha, \beta \in \mathbb{C}. \tag{2.35}$$

Coefficients α, β are called **probability amplitudes**. The state vector needs to be normalized

$$\||\psi\rangle\|^2 = \langle\psi|\psi\rangle = 1 \tag{2.36}$$

which means that $|\alpha|^2 + |\beta|^2 = 1$ (naturally, since the total probability of the system must be 1).

It should be noted that when every probability amplitude is multiplied by the same phase factor $e^{i\theta}$, then the resulting state is equivalent to the starting state. For example the following two states are equivalent:

$$\begin{aligned} |\psi\rangle &= \alpha\,|0\rangle + \beta\,|1\rangle \\ e^{i\theta}\,|\psi\rangle &= e^{i\theta}\alpha\,|0\rangle + e^{i\theta}\beta\,|1\rangle \end{aligned} \tag{2.37}$$

In this case $e^{i\theta}$ is called a **global phase factor**. In contrast, **relative phase factors**, in which case every probability amplitude is multiplied by a different phase factor, can lead to physically distinguishable states. The resulting state is not equivalent to the starting state in the case of relative phase factors.

2.2.5.2 Second Axiom: Time Evolution of a closed Quantum System

A quantum system that does not interact with any other system is called a closed system. Closed systems at time t are represented by state vectors $|\psi(t)\rangle$. At time t_0 the state vector is $|\psi(t_0)\rangle$. The second axiom of quantum mechanics states that the time evolution of a closed system can be described with unitary operators $U(t, t_0)$ as:

$$|\psi(t)\rangle = U(t, t_0)\,|\psi(t_0)\rangle \tag{2.38}$$

2.2.5.3 Third Axiom: Measurements in Quantum Mechanics

In many instances, it is desirable to determine the state of a quantum system. To achieve this, we must perform a measurement of an observable of the system. For such a measurement, a measurement device that interacts with the system is required. Due to this interaction with the measurement device, the system can no longer be considered closed. Therefore, the second axiom does not apply in the case of a

measurement. The third axiom describes the behavior of the system when such a measurement occurs.

The state of the system is described by state vectors within a Hilbert space. These state vectors can be realized as one of N possible distinct quantum states $|1\rangle, |2\rangle, \ldots, |N\rangle$. The quantum system can be found in one of these distinct states. A measurement device interacts with the system and yields a measurement outcome of one of these states. Since these states are completely distinct and different from each other, the respective state vectors are orthogonal to each other and they form an orthonormal basis for the Hilbert space. A general state $|\psi\rangle$ can therefore be expressed as a linear combination of these states:

$$|\psi\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle \tag{2.39}$$

The measurement axiom of quantum mechanics provides the probability of obtaining a specific state $|i\rangle$ being the outcome of a measurement. It can be strictly formulated as follows:

"For a quantum system in state $|\psi\rangle = \sum_{i=1}^{N} \alpha_i |i\rangle$ defined by the orthonormal basis $\{|i\rangle\} \in \mathcal{H}$, it is possible to perform a measurement with respect to this basis. The outcome of the measurement will be one of the possible states $|i\rangle$ with a probability of $|\alpha_i|^2$. After the measurement the system collapses probabilistically to the corresponding state $|i\rangle$".

2.2.5.4 Fourth Axiom: Composite Quantum Systems

The fourth axiom of quantum mechanics describes the state of a composite quantum system. It states that the Hilbert space of a composite system, formed by n subsystems, is the tensor product of the Hilbert spaces of the individual components. If n independent quantum systems with respective state vectors $|\psi_i\rangle \in \mathcal{H}_i, i = 1, 2, \ldots, n$ are combined, the state vector $|\psi\rangle$ of the composite system is the tensor product:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle, \ |\psi\rangle \in \mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_n \tag{2.40}$$

In the case of quantum computing with two-level systems, the composite system of n quantum subsystems is part of a 2^n-dimensional Hilbert space. Importantly, the state vector $|\psi\rangle$ of space $\mathcal{H}$ cannot always be represented as a simple tensor product of vectors $|\psi_i\rangle \in \mathcal{H}_i$. This form is valid only for subsystems that have been prepared independently from each other. In that case, the state of the composite quantum system is called a **product state** or **separable state**. To illustrate this, consider the following state of a two-level system:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \tag{2.41}$$

The states of the two subsystems are separable and the complete state of the composite system can be expressed as a simple tensor product:

$$|\psi\rangle = |0\rangle \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \tag{2.42}$$

When individual quantum systems interact during their initialization, the resulting composite state cannot be represented as a simple tensor product of independent subsystem states. Instead, the composite system

can be expressed as a superposition of product states:

$$|\psi\rangle = \sum_i c_i \left|\psi_1^{(i)}\right\rangle \otimes \left|\psi_2^{(i)}\right\rangle \otimes \ldots \otimes \left|\psi_n^{(i)}\right\rangle \tag{2.43}$$

States that exhibit this property are defined as **entangled states**. The defining characteristic of entanglement is **non-separability**, meaning that the state of the whole system is well-defined, yet the state of its constituent subsystems cannot be described independently. This phenomenon is a direct consequence of the fourth axiom and serves as a fundamental resource for quantum computing.

To better understand entangled states, we introduce a group of four maximally entangled states, which are frequently used in quantum computing, for a composite two-level system. These are known as **Bell states**. The Bell states form an orthonormal basis for the 4-dimensional Hilbert space and are defined as:

$$\begin{aligned} \left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ \left|\Psi^+\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad \left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{2.44}$$

It is evident that none of these states can be written as a simple tensor product. The implications of entanglement become most apparent when considering measurements. We extend the notion of measurement to include **partial measurements**, where an observable is measured on a single subsystem while the others remain unmeasured.

Consider a composite system in the entangled superposition described in equation (2.43). If we perform a partial measurement on the k-th subsystem and obtain the result i, the state of the composite system collapses to the corresponding state:

$$\left|\psi_1^{(i)}\right\rangle \otimes \left|\psi_2^{(i)}\right\rangle \otimes \ldots \otimes \left|\psi_n^{(i)}\right\rangle \tag{2.45}$$

To better understand this, we can use the Bell state $|\Phi^+\rangle$ as an example. A measurement performed solely on the first qubit (subsystem A) yields outcome $|0\rangle$ or $|1\rangle$ with equal probability (50%). This measurement also determines the state of the second qubit (subsystem B) with absolute certainty, regardless of whether B has been measured or not. If A is found to be $|0\rangle$, B instantly becomes $|0\rangle$ and if A is found to be $|1\rangle$, B instantly becomes $|1\rangle$. This happens irrespectively of the distance between the subsystems, which may be large. The collapse manifests simultaneously for both subsystems. Nevertheless, no information is transmitted between the subsystems and no form of faster-than-light signalling occurs.

2.3 The qubit

We know from classical computing that the fundamental unit of information is represented by a bit, which takes two possible values 0 and 1. This concept extends to quantum computing. In this case the fundamental unit of information is the **qubit** (quantum bit). A qubit is represented by a vector in a two-dimensional complex Hilbert space, describing the state of a quantum system. The computational basis

of the Hilbert space consists of the unit vectors $|0\rangle, |1\rangle \in \mathcal{H}^2$:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.46}$$

Physically, a qubit may correspond to the spin of an atom, the polarization of a photon or any other two-state quantum system that meets the following requirements:

(i) It can be initialized to a well-defined state.

(ii) It must be possible to implement a universal set of unitary operations acting on the qubit.

(iii) The state of the qubit can be measured with respect to the computational basis $\{|0\rangle, |1\rangle\}$.

These requirements are consistent with the fundamental criteria proposed by DiVincenzo for physical implementation of quantum information processing [19].

As previously discussed, a qubit belongs to the Hilbert space $\mathcal{H}^2$, which is spanned by the orthonormal basis vectors $\{|0\rangle, |1\rangle\}$. Consequently, a qubit $|q\rangle$ can be written as:

$$|q\rangle = \alpha |0\rangle + \beta |1\rangle, \ \alpha, \beta \in \mathbb{C} \tag{2.47}$$

where α and β are the probability amplitudes for basis states $|0\rangle$ and $|1\rangle$, respectively. Unlike the classical bit which is either a 0 or a 1, the qubit exists in a superposition of $|0\rangle$ and $|1\rangle$. Since α and β can be any complex number (provided that $|\alpha|^2 + |\beta|^2 = 1$), there is an infinite number of possible states for a qubit. Therefore, it could be argued that a single qubit contains an infinite amount of information. However, to extract any classical information from a qubit, we must perform a measurement, which destroys the superposition and the state of the qubit collapses to either $|0\rangle$ or $|1\rangle$.

2.3.1 The Bloch Sphere

To better understand qubits, we can try to visualize them. First, let us consider the general qubit state:

$$|q\rangle = \alpha |0\rangle + \beta |1\rangle \tag{2.48}$$

The probability amplitudes α and β are complex numbers. The polar representation of a complex number c can be expressed as:

$$c = re^{i\phi} \tag{2.49}$$

where r is the norm of the complex number and $e^{i\phi}$ encodes the phase. The qubit $|q\rangle$ is normalized, meaning that:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.50}$$

Recalling that

$$\sin^2 x + \cos^2 x = 1 \tag{2.51}$$

we can rewrite α and β as:

$$\alpha = e^{i\gamma} \cos\frac{\theta}{2}, \quad \beta = e^{i\delta} \sin\frac{\theta}{2} \tag{2.52}$$

The qubit $|q\rangle$ can now be expressed as:

$$|q\rangle = e^{i\gamma} \cos\frac{\theta}{2} |0\rangle + e^{i\delta} \sin\frac{\theta}{2} |1\rangle \tag{2.53}$$

We factor out $e^{i\gamma}$ ($\phi = \delta - \gamma$):

$$|q\rangle = e^{i\gamma}(\cos\frac{\theta}{2} |0\rangle + e^{i\phi} \sin\frac{\theta}{2} |1\rangle) \tag{2.54}$$

Finally, since the global phase factor has no observable effect on a measurement, we arrive at the generalized qubit $|q\rangle$ expression:

$$|q\rangle = \cos\frac{\theta}{2} |0\rangle + e^{i\phi} \sin\frac{\theta}{2} |1\rangle, \quad (0 \leq \theta \leq \pi, 0 \leq \phi \leq 2\pi) \tag{2.55}$$

Every pure qubit state can be mapped to a point on the surface of a unit sphere in $\mathbb{R}^3$, known as the **Bloch sphere**. On the Bloch sphere, a qubit is represented as a unit vector originating from the center, whose orientation is defined by the angles θ and ϕ. Antipodal points on the Bloch sphere correspond to orthogonal qubit states,which define a basis of the two-dimensional Hilbert space. Consequently, there is an infinite number of orthonormal bases in $\mathcal{H}^2$. Three of the most common ones correspond to the intersections of the axes with the sphere. Note that the generalized qubit expression (2.55) is used for the following calculations:

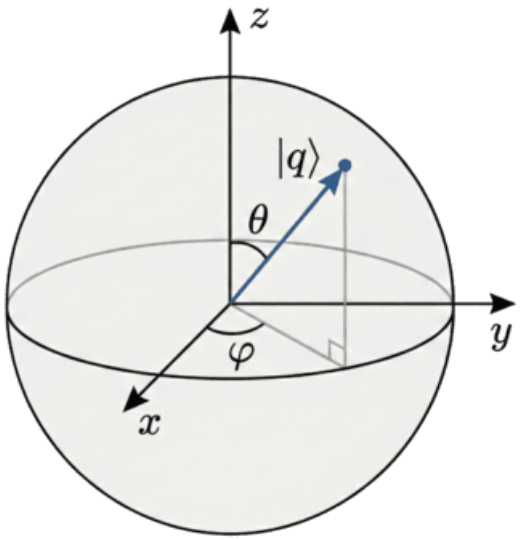

Figure 2.1: A qubit on the Bloch sphere

The **Z**-axis intercepts the sphere at its poles. At the Z^+ intersection, both angles θ and ϕ are equal to 0, resulting in state $|0\rangle$. At the Z^- intersection, angle θ is equal to π and angle ϕ is equal to 0, resulting in state $|1\rangle$. Qubits $|0\rangle$ and $|1\rangle$ are eigenvectors of the Pauli-Z operator with eigenvalues +1 and -1, respectively, and as we already discussed, form the canonical basis in quantum computing.

For the first **X**-axis intersection point X^+, angle θ is equal to $\frac{\pi}{2}$ and ϕ is equal to 0, resulting in state:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{2.56}$$

At the X^- intersection, angle θ is equal to $\frac{\pi}{2}$ and angle ϕ is equal to π, resulting in state:

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.57}$$

Qubits $|+\rangle$ and $|-\rangle$ are eigenvectors of the Pauli-X operator with eigenvalues +1 and -1, respectively, and form another orthonormal basis of $\mathcal{H}^2$.

For the first **Y**-axis intersection point Y^+, both angles θ and ϕ are equal to $\frac{\pi}{2}$, resulting in state:

$$|i+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \tag{2.58}$$

At the Y^- intersection, angle θ is equal to $\frac{\pi}{2}$ and angle ϕ is equal to $\frac{3\pi}{2}$, resulting in state:

$$|i-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle) \tag{2.59}$$

Qubits $|i+\rangle$ and $|i-\rangle$ are eigenvectors of the Pauli-Y operator with eigenvalues +1 and -1, respectively, and form another orthonormal basis of $\mathcal{H}^2$.

2.3.2 Quantum Registers

Let us consider a classical register consisting of 3 bits. The number of possible values that can be represented by such a register is $2^3 = 8$. At any given time, the register is set to one of those values, for example $110_2 = 6_{10}$. This concept can extend to quantum computing with the introduction of **quantum registers**. A quantum register of 3 qubits spans a Hilbert space of dimension $2^3 = 8$. The quantum register state is described by the tensor product of the register's qubits. Following the same example, if $|q_1\rangle$ and $|q_2\rangle$ are set to $|1\rangle$ and $|q_3\rangle$ is set to $|0\rangle$, the quantum register $|r\rangle$ is formed as:

$$|r\rangle = |q_1\rangle \otimes |q_2\rangle \otimes |q_3\rangle = |q_1 q_2 q_3\rangle = |110\rangle = |6\rangle \tag{2.60}$$

In this example, all qubits are set to one of the basis states $|0\rangle$ or $|1\rangle$, and the resulting quantum register appears identical to the classical one. However, unlike classical bits, qubits can exist in a superposition of $|0\rangle$ and $|1\rangle$. Let us consider that the first qubit $|q_1\rangle$ is set to the superposition :

$$|q_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{2.61}$$

The state of the register $|r\rangle$ is now:

$$|r\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |110\rangle) = \frac{1}{\sqrt{2}}(|2\rangle + |6\rangle) \tag{2.62}$$

The states $|2\rangle$ and $|6\rangle$ exist within the quantum register simultaneously, a phenomenon impossible for a classical register. We can further generalize the state of a 3-qubit quantum register by initializing all qubits to the superposition state defined in (2.61). The generalized state of the quantum register $|R_3\rangle$ is:

$$\begin{aligned} |R_3\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \\ &= \frac{1}{\sqrt{2^3}} \sum_{x=0}^{7} |x\rangle \end{aligned} \tag{2.63}$$

It is now evident that an n n-qubit quantum register spans a Hilbert space of dimension 2^n and when all qubits are in superposition, the register describes a state involving all 2^n basis states simultaneously, expressed as:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \tag{2.64}$$

2.4 Quantum Gates

In classical circuits, a series of logical gates, such as NOT or AND, are used to produce an output bit based on their respective truth tables. In quantum circuits we use **quantum gates**. These gates are unitary operators that act on a qubit or a quantum register and transform its state. We can express the effect of a quantum gate G on a quantum register $|r_0\rangle$ as:

$$G\,|r_0\rangle = |r_1\rangle \tag{2.65}$$

2.4.1 Single Qubit Gates

These gates act on a single qubit $|q_0\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and transform it into state $|q_1\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$. The schematic representation of a general single qubit gate G is:

Figure 2.2: Schematic representation of a general single qubit gate G.

We will now examine some of the most useful single qubit gates.

2.4.1.1 Identity Gate

The identity gate (denoted I) acts on a qubit without transforming it. The matrix representation of the identity gate is:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.66}$$

The schematic representation is:

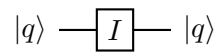

Figure 2.3: Schematic representation of the identity gate.

2.4.1.2 Quantum NOT Gate

The quantum NOT gate (denoted X) maps state $|0\rangle$ to state $|1\rangle$ and vice versa. The matrix expression of the NOT gate is:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2.67}$$

The schematic representation is:

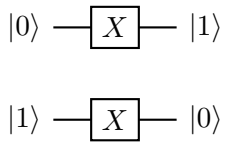

Figure 2.4: Schematic representation of the NOT gate on basis states $|0\rangle$ and $|1\rangle$.

Assuming that a qubit $|q\rangle$ is in a superposition state $|q\rangle = \alpha|0\rangle + \beta|1\rangle$, the NOT gate acts linearly on both basis states and transforms $|q\rangle$ as follows:

$$X|q\rangle = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle \tag{2.68}$$

The schematic representation is:

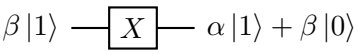

Figure 2.5: Schematic representation of the NOT gate acting on superposition state $|q\rangle$.

2.4.1.3 Hadamard Gate

The Hadamard gate (denoted H) is represented by the following matrix:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2.69}$$

The Hadamard gate is used to transform the computational basis states $|0\rangle$ and $|1\rangle$ into superposition states. It acts on state $|0\rangle$ as follows:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \tag{2.70}$$

and on state $|1\rangle$:

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \tag{2.71}$$

The schematic representation is:

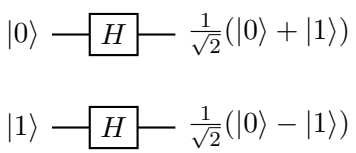

Figure 2.6: Schematic representation of the Hadamard gate on basis states $|0\rangle$ and $|1\rangle$.

2.4.2 Multi Qubit Gates

We can define quantum gates that act on more than one qubit. Such gates are useful for creating entanglement between qubits.

2.4.2.1 Quantum controlled-NOT (CNOT) gate

The controlled-NOT gate acts on two qubits, which are vectors of $\in \mathcal{H}^4$, where the basis is expressed as:

$$\begin{aligned} |00\rangle &= \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \quad |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \\ |10\rangle &= \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \quad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \end{aligned} \tag{2.72}$$

The first qubit of the CNOT gate is called the **control qubit** and the second qubit is called the **target qubit**. The CNOT gate does not affect the control qubit. The target qubit is transformed depending on the control qubit's state. If the control qubit's state is $|0\rangle$ the target qubit is not transformed. On the contrary, if the control qubit's state is $|1\rangle$, then the target qubit is flipped from state $|0\rangle$ to $|1\rangle$ and vice versa. The CNOT gate is the quantum equivalent of the classical **XOR** gate. We can define a CNOT gate's action on two qubits $|c\rangle$, $|t\rangle$ as follows:

$$CNOT(|c\rangle\,|t\rangle) = |c\rangle\,|c \oplus t\rangle \tag{2.73}$$

where $\oplus$ denotes addition modulo 2. The schematic representation is:

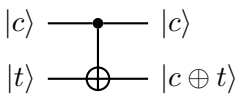

Figure 2.7: Schematic representation of the CNOT gate.

The CNOT gate's truth table is the following:

Table 2.1: CNOT's truth table

$\|c\rangle$	$\|t\rangle$	$\|c \oplus t\rangle$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

Let us consider the case where the target qubit is in a superposition state $\alpha\,|0\rangle + \beta\,|1\rangle$. Assuming that the control qubit's state is $|1\rangle$, the CNOT gate's action on the two-qubit system is:

$$CNOT[|1\rangle\otimes(\alpha\,|0\rangle+\beta\,|1\rangle)] = CNOT(\alpha\,|10\rangle+\beta\,|11\rangle) = \alpha\,|11\rangle+\beta\,|10\rangle = |1\rangle\otimes(\alpha\,|1\rangle+\beta\,|0\rangle) \quad (2.74)$$

2.4.2.2 Toffoli Gate (CCNOT)

The Toffoli or controlled-controlled-NOT (CCNOT) gate acts on three qubits. Both the first and the second qubit of the CCNOT gate act as control qubits and the third qubit is the target qubit. The CCNOT gate does not affect the control qubits. Both control qubits need to be in state $|1\rangle$ for the target qubit's state to be reversed. We can define a CCNOT gate's action on three qubits $|c_1\rangle, |c_2\rangle, |t\rangle$ as follows:

$$CCNOT(|c_1\rangle\,|c_2\rangle\,|t\rangle) = |c_1\rangle\,|c_2\rangle\,|(c_1 \wedge c_2) \oplus t\rangle \quad (2.75)$$

where $\wedge$ denotes the logical AND operation. The schematic representation is:

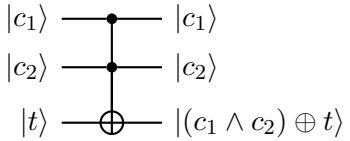

Figure 2.8: Schematic representation of the CCNOT gate.

The CCNOT gate's truth table is the following:

Table 2.2: CCNOT gate's truth table

Input State			**Output State**		
$\|c_1\rangle$	$\|c_2\rangle$	$\|t\rangle$	$\|c_1\rangle$	$\|c_2\rangle$	$\|(c_1 \wedge c_2) \oplus t\rangle$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

2.5 Quantum Circuits

Let us consider a quantum register of n qubits initialized to the input state $|\psi\rangle$. By applying a series of quantum gates we can transform the state $|\psi\rangle$ to a target state $|\psi'\rangle$. This sequence of gate operations constitutes a **quantum circuit**. To better understand the concept of quantum circuits, we can construct and analyze such a circuit step-by-step as an example.

Step 1: The register is initialized to a state $|\psi\rangle$. Let us take $|\psi\rangle = |01\rangle$:

Figure 2.9: Step 1: Initialization of the two-qubit quantum register to the state $|01\rangle$.

Step 2: A Hadamard gate is applied to both qubits:

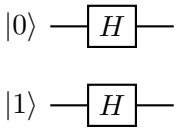

Figure 2.10: Step 2: Applying Hadamard gates to both qubits.

Step 3: A CNOT gate with the first qubit as the control and the second qubit as the target is applied:

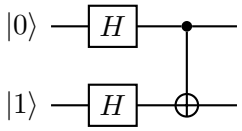

Figure 2.11: Step 3: Applying a CNOT gate with the first qubit as control and the second as target.

Step 4: A Hadamard gate is applied to the first qubit:

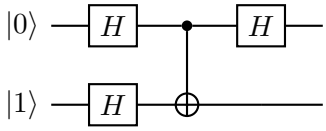

Figure 2.12: Step 4: Applying a Hadamard gate to the first qubit.

Note that in Step 4, the application of the Hadamard gate to the first qubit is accompanied by the application of the identity gate I to the second qubit for mathematical consistency of the tensor product formalism. Nevertheless, we can omit the identity gate from the schematic, as it does not affect the qubit it is applied to. This concludes the construction of the quantum circuit.

Having constructed the quantum circuit, we now proceed to evaluate it. To do so, we will compute the state of the system step-by-step.

Step 1: The register is initialized to state:

$$|\psi_0\rangle = |0\rangle \otimes |1\rangle = |01\rangle \tag{2.76}$$

Step 2: A Hadamard gate is applied to both qubits:

$$\begin{aligned} |\psi_1\rangle &= (H \otimes H)\,|\psi_0\rangle = H\,|0\rangle \otimes H\,|1\rangle \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \end{aligned} \tag{2.77}$$

Step 3: A CNOT gate with the first qubit as control and the second qubit as target is applied:

$$\begin{aligned} |\psi_2\rangle &= CNOT\,|\psi_1\rangle \\ &= \frac{1}{2}(CNOT\,|00\rangle - CNOT\,|01\rangle + CNOT\,|10\rangle - CNOT\,|11\rangle) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle) \end{aligned} \tag{2.78}$$

Step 4: A Hadamard gate is applied to the first qubit:

$$\begin{aligned} |\psi_3\rangle &= (H \otimes I)\,|\psi_2\rangle \\ &= \frac{1}{2}[(H\,|0\rangle \otimes I\,|0\rangle) - (H\,|0\rangle \otimes I\,|1\rangle) + (H\,|1\rangle \otimes I\,|1\rangle) - (H\,|1\rangle \otimes I\,|0\rangle)] \\ &= \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle) = \frac{1}{\sqrt{2}}[|1\rangle \otimes (|0\rangle - |1\rangle)] \end{aligned} \tag{2.79}$$

This concludes the step-by-step evaluation of the quantum circuit shown in Fig. 2.12.

Note that, in many instances in a quantum circuit we want to take a measurement of a qubit. The schematic representation of a measurement is the following:

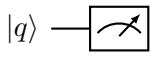

Figure 2.13: Schematic representation of a single qubit q measurement.

Quantum circuits form the fundamental framework for the implementation of quantum algorithms.

2.6 Quantum Algorithms

Having introduced the principles of quantum gates and quantum circuits, we are now ready to discuss **quantum algorithms**. Quantum algorithms are often presented as more efficient alternatives to their classical counterparts. They exploit fundamental phenomena of quantum mechanics, such as superposition and entanglement. In this section, we present a few of the most fundamental quantum algorithms.

2.6.1 Deutsch's Algorithm

The first algorithm to demonstrate a quantum computational advantage was proposed by Deutsch in 1985 [5]. Deutsch's algorithm solves the following problem:

"Given a boolean function $f : \{0, 1\} \to \{0, 1\}$, calculate if f is constant or balanced".

A function is called constant if $f(0) = f(1)$ and balanced if $f(0) \neq f(1)$. A classical computer would solve the following problem like this:

i Calculate $f(0)$.

ii Calculate $f(1)$.

iii Compare $f(0)$ and $f(1)$.

Two computations of f are needed for solving the problem with a classical computer. Using Deutsch's algorithm, the problem can be solved with only **one** oracle evaluation.

Before we introduce the algorithm, we define the unitary oracle gate U_f. The action of U_f on a two-qubit register is defined as follows:

$$U_f(|x\rangle\,|y\rangle) = |x\rangle\,|y \oplus f(x)\rangle \tag{2.80}$$

The schematic representation is:

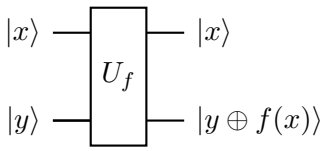

Figure 2.14: Schematic representation of the oracle gate U_f.

Having defined the oracle gate U_f, we can now introduce Deutsch's algorithm. The quantum circuit is the following:

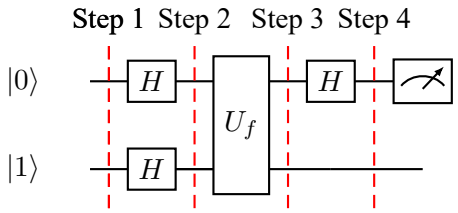

Figure 2.15: Circuit diagram of Deutsch's Algorithm.

We will now implement Deutsch's algorithm step-by-step.

Step 1: The system is initialized to state:

$$|\psi_0\rangle = |01\rangle = |xy\rangle \tag{2.81}$$

Step 2: A Hadamard gate is applied to both qubits:

$$\begin{aligned} |\psi_1\rangle &= (H \otimes H)(|0\rangle \otimes |1\rangle) \\ &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \end{aligned} \tag{2.82}$$

Step 3: The oracle gate U_f is applied:

$$\begin{aligned} |\psi_2\rangle &= U_f\,|\psi_1\rangle \\ &= \frac{1}{2}\,|0\rangle\,(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + \frac{1}{2}\,|1\rangle\,(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle) \end{aligned} \tag{2.83}$$

Recalling that $f(0)$ and $f(1)$ can only take values in $\{0, 1\}$, the expression can be further simplified using:

$$|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle), \quad x = \{0, 1\} \tag{2.84}$$

The state of the system can now be expressed as:

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{2}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}(-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2}}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right] \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \frac{1}{\sqrt{2}}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right] \otimes |-\rangle\end{aligned} \tag{2.85}$$

Note that the left term of the tensor product is the value of the first qubit (x) and the right term the value of the second qubit (y). The state of the second qubit remains unchanged by the application of the oracle gate. This effect is known as **phase kickback**. Since the target (y) qubit is in the eigenstate $|-\rangle$, the oracle encodes the function's value $f(x)$ directly into the phase of the control (x) qubit.

Step 4: A Hadamard gate is applied to the first qubit:

$$\begin{aligned}|\psi_3\rangle = (H \otimes I)|\psi_2\rangle &= \frac{1}{\sqrt{2}}H[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle] \otimes I|-\rangle \\ &= \frac{1}{\sqrt{2}}[(-1)^{f(0)}H|0\rangle + (-1)^{f(1)}H|1\rangle] \otimes |-\rangle \\ &= \frac{1}{\sqrt{2}}\left[(-1)^{f(0)}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + (-1)^{f(1)}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right] \otimes |-\rangle \\ &= \left[\frac{1}{2}\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \frac{1}{2}\left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right] \otimes |-\rangle\end{aligned} \tag{2.86}$$

Measurement: A measurement is performed on the first qubit

$$|x\rangle = \frac{1}{2}\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \frac{1}{2}\left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle \tag{2.87}$$

We can distinguish two possible outcomes, based on the nature of the function f:

i If f is constant ($f(0) = f(1)$), then $(-1)^{f(0)}$ and $(-1)^{f(1)}$ are equal (± 1). In this case, the probability amplitude of $|0\rangle$ is $\pm$ 1 and the probability amplitude of $|1\rangle$ is 0. In other words, a measurement that yields the result $|0\rangle$ implies that f is constant.

ii If f is balanced ($f(0) \neq f(1)$), then one of $(-1)^{f(0)}$ and $(-1)^{f(1)}$ is equal to 1 and the other is equal to -1. In this case, the probability amplitude of $|0\rangle$ is 0 and the probability amplitude of $|1\rangle$ is $\pm$ 1. In other words, a measurement that yields the result $|1\rangle$ implies that f is balanced.

Note that in 1992, Deutsch's algorithm was generalized for n input qubits with the introduction of the **Deutsch-Jozsa algorithm** [20] .

2.6.2 Simon's Algorithm

Simon's algorithm, named after Daniel Simon who proposed it in 1994 [21], determines the hidden period s of a function $f : \{0,1\}^n \to \{0,1\}^n$:

$$f(x) = f(y) \iff x = y \text{ or } x = y \oplus s \tag{2.88}$$

where $s \neq 0$ is the hidden period of f. The classical query complexity of the problem is exponential in n. With Simon's algorithm, the quantum query complexity is linear, $O(n)$.

Before we introduce Simon's algorithm, we define the oracle gate U_f acting on two n-qubit registers as follows:

$$U_f \left|x\right\rangle_n \left|y\right\rangle_n = \left|x\right\rangle_n \left|y \oplus f(x)\right\rangle_n \tag{2.89}$$

The circuit diagram of Simon's algorithm is the following:

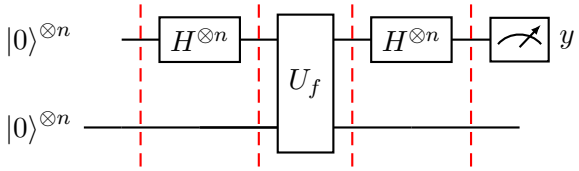

Figure 2.16: Circuit diagram of Simon's algorithm.

We will now implement Simon's algorithm step-by-step.

Step 1: The system is initialized to state:

$$\left|\psi_0\right\rangle = \left|0\right\rangle_n \left|0\right\rangle_n \tag{2.90}$$

Note that $\left|0\right\rangle_n$ represents a register of n qubits.

Step 2: An n-qubit Hadamard transform $H^{\otimes n}$ is applied to the first register:

$$\left|\psi_1\right\rangle = (H^{\otimes n} \otimes I^{\otimes n})(\left|0\right\rangle_n \left|0\right\rangle_n) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \left|x\right\rangle \left|0\right\rangle_n \tag{2.91}$$

Step 3: The oracle gate U_f is applied:

$$\left|\psi_2\right\rangle = U_f \left|\psi_1\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \left|x\right\rangle \left|f(x)\right\rangle \tag{2.92}$$

A measurement on the second register yields a value $f(x_0)$. Since f is periodic with a period s, $f(x_0) = f(x_0 \oplus s)$. Consequently, a measurement on the second register collapses the first register into the equal superposition:

$$\left|x\right\rangle = \frac{1}{\sqrt{2}}(\left|x_0\right\rangle + \left|x_0 \oplus s\right\rangle) \tag{2.93}$$

To better understand the following steps, note that the application of an $H^{\otimes n}$ Hadamard transform to an n-qubit register $\left|r\right\rangle$, $r \in \{0,1\}^n$ results in the following:

$$H^{\otimes n} \left|r\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{r \cdot y} \left|y\right\rangle \tag{2.94}$$

where $r \cdot y = r_0 y_0 \oplus r_1 y_1 \oplus \ldots \oplus r_{n-1} y_{n-1}$

Step 4: An n-qubit Hadamard transform $H^{\otimes n}$ is again applied to the first register:

$$\begin{aligned}
|\psi_3\rangle = H^{\otimes n}|x\rangle &= \frac{1}{\sqrt{2}}\left(H^{\otimes n}|x_0\rangle + H^{\otimes n}|x_0 \oplus s\rangle\right) \\
&= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}\left((-1)^{x_0\cdot y}|y\rangle + (-1)^{(x_0\oplus s)\cdot y}|y\rangle\right) \\
&= \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}\left[(-1)^{x_0\cdot y} + (-1)^{(x_0\oplus s)\cdot y}\right]|y\rangle \\
&= \frac{1}{\sqrt{2^{n+1}}}\sum_{y\in\{0,1\}^n}\left[(-1)^{x_0\cdot y}(1 + (-1)^{s\cdot y})\right]|y\rangle
\end{aligned} \tag{2.95}$$

Measurement: It is evident that $s \cdot y$ can either be equal to 0 or 1. For $s \cdot y = 1$, the amplitude of $|y\rangle$ vanishes. Thus, a measurement on the first register yields a value of y, which satisfies $y \cdot s = 0$. We perform $O(n)$ measurements, yielding different y values, $y_1, y_2, \ldots, y_n$. We can therefore construct a system of linear equations:

$$\begin{cases} y_1 \cdot s = 0 \\ y_2 \cdot s = 0 \\ \vdots \\ y_n \cdot s = 0 \end{cases} \tag{2.96}$$

A classical computer is then used to solve the resulting linear system and determine the hidden period s.

2.6.3 Quantum Fourier Transform

The Quantum Fourier Transform (QFT) is the quantum analogue of the classical Discrete Fourier Transform (DFT) and constitutes a fundamental building block of many quantum algorithms, including phase estimation and Shor's algorithm. Its importance does not stem from directly providing the full Fourier spectrum of a quantum state through measurement, but rather from enabling the controlled manipulation of relative phases in quantum superpositions. These phase relationships can then be exploited through quantum interference in subsequent computational steps.

First, let us recall the Discrete Fourier Transform (DFT). Let $x = [x_0, x_1, \ldots, x_{N-1}]$ be a vector of complex numbers, with $x_j \in \mathbb{C}$. The DFT of x is the vector $y = \text{DFT}(x)$ with components

$$y_k = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} x_j e^{i2\pi jk/N} \tag{2.97}$$

The DFT maps a discrete signal from the time domain to the frequency domain.

Let us now derive the quantum analogue of DFT. Consider an n-qubit register, with Hilbert space dimension $N = 2^n$. Any pure state of the register can be written in the computational basis as

$$|\phi\rangle = \sum_{k=0}^{N-1} \phi_k |k\rangle \tag{2.98}$$

where $|k\rangle$ denotes the computational basis state corresponding to the binary expansion of the integer k, and $\phi_k \in \mathbb{C}$ are complex amplitudes. The QFT of a computational basis state $|k\rangle$ is defined as a unitary operator $\mathcal{F}_Q$ acting on $|k\rangle$ as follows:

$$\mathcal{F}_Q |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{i2\pi kj/N} |j\rangle \tag{2.99}$$

The QFT of the n-qubit register's state in eq. (2.98) is the state $|\psi\rangle \in \mathcal{H}$, defined as:

$$|\psi\rangle = \mathcal{F}_Q |\phi\rangle = \sum_{k=0}^{N-1} \phi_k \mathcal{F}_Q |k\rangle \tag{2.100}$$

By linearity:

$$|\psi\rangle = \mathcal{F}_Q |\phi\rangle = \sum_{j=0}^{N-1} \psi_j |j\rangle , \tag{2.101}$$

with amplitudes

$$\psi_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \phi_k e^{i2\pi kj/N} \tag{2.102}$$

Note that the output amplitudes ψ_j are precisely the classical DFT of the input amplitudes ϕ_k. To better understand the QFT, consider a simple one-qubit register ($N = 2$). The QFT for state $|0\rangle$ is the following:

$$\mathcal{F}_Q |0\rangle = \frac{1}{\sqrt{2}} \sum_{j=0}^{2-1} e^{i2\pi 0j/2} |j\rangle = \frac{1}{\sqrt{2}} (e^0 |0\rangle + e^0 |1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \tag{2.103}$$

For state $|1\rangle$, respectively:

$$\mathcal{F}_Q |1\rangle = \frac{1}{\sqrt{2}} \sum_{j=0}^{2-1} e^{i2\pi 1j/2} |j\rangle = \frac{1}{\sqrt{2}} (e^0 |0\rangle + e^{i\pi} |1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \tag{2.104}$$

The QFT action over a basis state yields a superposition state of the basis vectors.

The inverse Quantum Fourier Transform is defined as the adjoint operator

$$\mathcal{F}_Q^\dagger |k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-i2\pi kj/N} |j\rangle \tag{2.105}$$

To obtain an efficient circuit implementation, we derive a factorized expression for $\mathcal{F}_Q |k\rangle$. Let $0 \leq k < 2^n$ be an integer, written in binary as:

$$k = k_1 k_2 \dots k_n = \sum_{\ell=1}^{n} k_\ell 2^{n-\ell}, \qquad k_\ell \in 0, 1. \tag{2.106}$$

The integer j is expressed as:

$$j = j_1 j_2 \dots j_n = \sum_{\ell=1}^{n} j_\ell 2^{n-\ell} \tag{2.107}$$

Using this binary expansion, the phase factor can be decomposed into a product of contributions from individual qubits. After straightforward algebra, we obtain:

$$\mathcal{F}_Q |k\rangle = \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{i2\pi k 2^{-1}} |1\rangle\right) \otimes \left(|0\rangle + e^{i2\pi k 2^{-2}} |1\rangle\right) \otimes \ldots \otimes \left(|0\rangle + e^{i2\pi k 2^{-n}} |1\rangle\right) \quad (2.108)$$

Thus, the QFT maps the basis state $|k\rangle$ to a product state of single qubits, each encoding a distinct phase of the form $e^{i2\pi k/2^j}$. Our goal is to implement these phases using elementary quantum gates. By analyzing the term $k/2^j$, we can distinguish between its integer and fractional components. The integer part corresponds to a global phase rotation of 2π, which has no observable physical consequence. As a result, only the fractional component of $k/2^j$ is relevant for the construction of the circuit. Let the integer k be written in binary form as shown in eq. (2.107). Then the ratio $k/2^j$ may be expanded as

$$\frac{k}{2^j} = \sum_{\ell=1}^{n} k_\ell 2^{n-\ell-j}. \quad (2.109)$$

The terms with negative powers of two constitute the fractional part of this expression, which we denote in binary notation as [18]

$$0.k_{n-j+1}k_{n-j+2}\ldots k_n. \quad (2.110)$$

Hence, the associated phase factor may be written as

$$e^{i2\pi k/2^j} = e^{i2\pi(0.k_{n-j+1}k_{n-j+2}\ldots k_n)}. \quad (2.111)$$

Using this representation, the QFT of a basis state $|k\rangle$, as shown in eq. (2.108) takes the form [18]:

$$\mathcal{F}_Q |k\rangle = \frac{1}{\sqrt{2^n}} \left[|0\rangle + e^{i2\pi(0.k_n)} |1\rangle\right] \otimes \left[|0\rangle + e^{i2\pi(0.k_{n-1}k_n)} |1\rangle\right] \otimes \cdots \otimes \left[|0\rangle + e^{i2\pi(0.k_1k_2\ldots k_n)} |1\rangle\right] \quad (2.112)$$

To implement this transformation as a quantum circuit, we consider how an individual qubit $|k_\ell\rangle$ of the register $|k_1\rangle |k_2\rangle \ldots |k_n\rangle$ must be transformed. From the expression above, the target state of qubit ℓ is

$$\mathcal{F}_Q |k_\ell\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i2\pi(0.k_\ell k_{\ell+1}\ldots k_n)} |1\rangle\right). \quad (2.113)$$

This phase factor may be decomposed as

$$e^{i2\pi(0.k_\ell k_{\ell+1}\ldots k_n)} = e^{i2\pi(0.k_\ell)} \cdot e^{i2\pi(0.0k_{\ell+1}\ldots k_n)}. \quad (2.114)$$

The first term satisfies

$$\frac{1}{\sqrt{2}} \left(|0\rangle + e^{i2\pi k_\ell/2} |1\rangle\right) = \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{k_\ell} |1\rangle\right), \quad (2.115)$$

which is precisely the action of a Hadamard gate applied to the qubit $|k_\ell\rangle$. The remaining phase contributions are generated through controlled phase-shift operations. We define the single-qubit phase rotation

gate

$$R_j = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^j} \end{pmatrix}. \tag{2.116}$$

R_ℓ acts non-trivially only when the control qubit is in state $|1\rangle$. R_ℓ multiplies the qubits $|1\rangle$ phase by a factor $e^{i2\pi(0.00\ldots k_\ell)_2}$.
The QFT is therefore implemented by the following procedure. Starting from the register $|k_1\rangle\,|k_2\rangle\ldots|k_n\rangle$:

- Apply a Hadamard gate to the most significant qubit.
- Apply controlled-$R_2, R_3, \ldots, R_n$ gates to the most significant qubit, controlled by the subsequent qubits.
- Repeat this process for each qubit of the register.
- Finally, apply swap gates to reverse the order of the qubits.

This sequence of operations produces exactly the state prescribed by the QFT, completing the circuit-level realization of $\mathcal{F}_Q$. The schematic representation of the QFT circuit structure is the following:

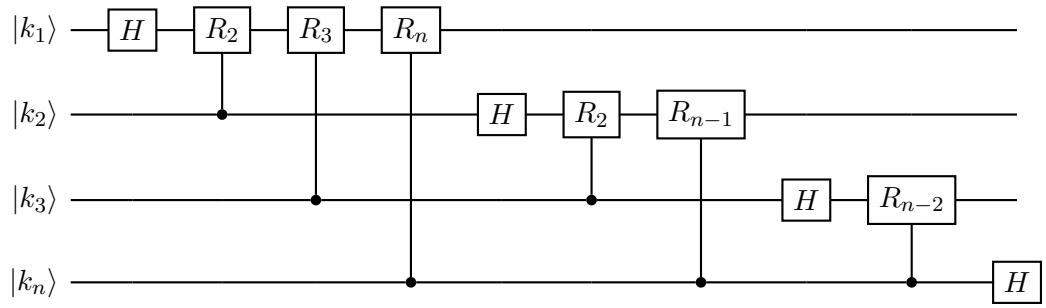

Figure 2.17: Circuit diagram of the Quantum Fourier Transform. Swap gates are omitted for clarity.

2.6.4 Shor's Algorithm

Public-key cryptography plays a fundamental role in modern information security, with the RSA cryptosystem [22] being one of the most widely deployed encryption schemes. The security of RSA relies on the computational difficulty of factoring large composite integers into their prime factors using classical algorithms. While integer factorization is believed to be intractable for sufficiently large numbers on classical computers, the advent of quantum computation fundamentally alters this assumption.

Shor's algorithm, introduced by Peter Shor in 1994 [6], is a quantum algorithm that solves the integer factorization problem in polynomial time on a quantum computer, fundamentally outperforming known classical algorithms.

Let us recall how the RSA code works. First, two random large prime numbers p and q are chosen. These numbers remain secret. The product n is then calculated:

$$n = pq \tag{2.117}$$

The Euler function $\phi(n) = (p-1)(q-1)$ is calculated. Then, an integer e is chosen such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. Finally, the integer d is calculated such that:

$$ed \equiv 1 \pmod{\phi(n)} \tag{2.118}$$

The public key of the RSA is (n, e) and the private key is d. Let us now examine how the RSA cryptography works. Alice wants to send a message (integer) $0 \leq m < n$ to Bob. Bob's public key is used to generate the cryptographic message c as:

$$c \equiv m^e \pmod{n}, \quad c \in \mathbb{Z}_n, \quad 0 \leq c < n \tag{2.119}$$

Bob's private key d is used to decipher c:

$$m \equiv c^d \pmod{n} \tag{2.120}$$

To get access to Bob's private key, a third party needs to factor n into a product of prime numbers, to calculate p and q. No efficient classical algorithm for integer factorization is currently known.

Having recalled the RSA cryptography, we can now introduce Shor's algorithm. Shor's algorithm exploits quantum superposition and interference to extract information about the period through measurement and classical post-processing. The algorithm consists of two parts: a classical reduction of the factorization problem to a period-finding problem, and a quantum subroutine to solve the latter.

The Classical Reduction: The problem of factoring the composite integer n can be reduced to the problem of finding the order (period) r of a randomly chosen element a modulo n. The procedure is as follows:

1. Choose a random integer a such that $1 < a < n$.
2. Calculate $\gcd(a, n)$.
   - If $\gcd(a, n) \neq 1$, then we have fortuitously found a non-trivial factor of n, and the problem is solved.
   - If $\gcd(a, n) = 1$, proceed to the next step.
3. Find the period r of the function:

   $$f(x) = a^x \pmod{n} \tag{2.121}$$

   The period r is the smallest positive integer such that $f(x + r) = f(x)$, or equivalently:

   $$a^r \equiv 1 \pmod{n} \tag{2.122}$$

   This step constitutes the computational bottleneck for classical algorithms and is addressed using a quantum computer.
4. Once r is determined, if r is even and $a^{r/2} \not\equiv -1 \pmod{n}$, then the prime factors p and q of n can

be computed as:

$$\gcd(a^{r/2} \pm 1, n) \tag{2.123}$$

The Quantum Period-Finding Subroutine: The quantum subroutine of Shor's algorithm is based on the Quantum Fourier Transform introduced in the previous section. To find the period r, we employ a quantum circuit using two registers. The first register (control register) consists of t qubits, such that the total number of states $Q = 2^t > n^2$. This choice of Q ensures sufficient precision for extracting the period r. The second register (target register) is used to store the function output $f(x)$.

1. The system is initialized to the state:

$$|\psi_0\rangle = |0\rangle^{\otimes t} |0\rangle^{\otimes L} \tag{2.124}$$

   where L is the number of qubits required to store n.

2. We apply Hadamard gates ($H^{\otimes t}$) to the first register, creating a uniform superposition of all integers x from 0 to $Q - 1$:

$$|\psi_1\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |0\rangle \tag{2.125}$$

3. We apply the unitary operator U_f, which performs the modular exponentiation $|x\rangle |y\rangle \to |x\rangle |y \oplus (a^x \pmod n)\rangle$. Since the second register is initially $|0\rangle$, the state becomes:

$$|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |a^x \pmod n\rangle \tag{2.126}$$

   At this point, the two registers are entangled. The function $f(x) = a^x \pmod n$ is periodic with period r, meaning $f(x) = f(x + r)$.

4. We measure the second register of the system. Let the measurement result be a value k. Because the qubits are entangled, the measurement of the second register determines the state of the first. The first register now contains only those inputs x' that satisfy the condition $f(x') = k$. We define the set A of these values as:

$$A = \{x' : a^{x'} \pmod n = k\} \tag{2.127}$$

   If $\|A\|$ denotes the number of elements in set A, then after the measurement, the total system state $|\psi_3\rangle$ is:

$$|\psi_3\rangle = \frac{1}{\sqrt{\|A\|}} \sum_{x' \in A} \left|x'\right\rangle \left|f(x')\right\rangle \tag{2.128}$$

   where $|f(x')\rangle = |k\rangle$ for all $x' \in A$.

5. We apply the Quantum Fourier Transform to the first register. The QFT operation is defined as:

$$QFT \left|x'\right\rangle = \frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} e^{\frac{2\pi i x' y}{Q}} |y\rangle \tag{2.129}$$

Thus, the state of the register $|\psi\rangle$ evolves to:

$$|\psi_4\rangle = \frac{1}{\sqrt{\|A\|}} \sum_{x' \in A} \left(\frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} e^{\frac{2\pi i x' y}{Q}} |y\rangle \right) \left| f(x') \right\rangle \tag{2.130}$$

Rearranging the sums, we get:

$$|\psi_4\rangle = \frac{1}{\sqrt{\|A\| \cdot Q}} \sum_{y=0}^{Q-1} \sum_{x' \in A} e^{\frac{2\pi i x' y}{Q}} |y\rangle \left| f(x') \right\rangle \tag{2.131}$$

6. We perform a measurement on the first register. The probability of obtaining a specific state $|y\rangle$ is given by the squared magnitude of its amplitude:

$$P(y) = \frac{1}{\|A\| \cdot Q} \left| \sum_{x' \in A} e^{\frac{2\pi i x' y}{Q}} \right|^2 \tag{2.132}$$

Substituting the periodic form of the elements in A ($x' = x_0 + jr$), the sum inside the modulus exhibits constructive interference when:

$$\frac{ry}{Q} \approx \lambda \Rightarrow y \approx \lambda \frac{Q}{r} \tag{2.133}$$

where λ is an integer.

7. The measurement of the first register yields an integer outcome y. Based on the interference pattern, the value $\frac{y}{Q}$ is, with high probability, a close approximation to the fraction $\frac{\lambda}{r}$, where λ is an integer. Specifically, the following inequality holds [18]:

$$\left| \frac{y}{Q} - \frac{\lambda}{r} \right| < \frac{1}{2Q} \tag{2.134}$$

Since Q is chosen such that $Q \geq n^2$, the **Continued Fractions Algorithm** [23] can be employed to determine the unique fraction $\frac{\lambda}{r}$ (and consequently the denominator r) that satisfies this condition.

8. Once a candidate period r is obtained from the continued fractions expansion, we classically verify if it satisfies $a^r \equiv 1 \pmod{n}$.

   - If the condition holds, the period r is found.
   - If the condition fails (or if $\gcd(\lambda, r) \neq 1$, leading to a factor of the true period), the quantum subroutine is repeated until a valid period is found.

Chapter 3: Protocols and Algorithms for Quantum Communications

3.1 Introduction

In the previous chapter, we explored the computational power of quantum systems and examined how quantum algorithms offer significant speedups over their classical counterparts. However, the potential of quantum mechanics extends beyond computation to the realm of information transmission. This chapter focuses on **Quantum Communication**.

Unlike classical bits, which can be easily copied and broadcasted, quantum states obey strict physical restrictions. We begin by proving the **No-Cloning Theorem**, a fundamental principle stating that an unknown quantum state cannot be perfectly duplicated. We will demonstrate how this theorem guarantees the security of **Quantum Key Distribution (QKD)**. Furthermore, we examine protocols that utilize entanglement as a resource for information transfer. We introduce **Quantum Teleportation**, a counter-intuitive protocol that allows the transmission of a quantum state from one location to another without the physical transfer of the particle itself. Finally, we discuss **Entanglement Swapping**, a mechanism that enables the entanglement of two particles that have never interacted, serving as a fundamental building block for the implementation of quantum repeaters and quantum networks.

3.2 The No-Cloning Theorem

The security of quantum key distribution relies heavily on a fundamental principle of quantum mechanics known as the **No-Cloning Theorem** [24]. This theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state.

3.2.1 Proof of the Theorem

Let us assume that there exists a universal quantum copying machine, represented by a unitary operator U, which can clone an arbitrary quantum state $|\psi\rangle$. To perform this operation, the machine requires two input registers:

1. **Data Register:** Contains the state $|\psi\rangle$ to be cloned.
2. **Target Register:** An ancillary qubit initialized to a standard blank state $|s\rangle$ (usually $|0\rangle$).

The action of the cloning operator U is defined as:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{3.1}$$

Since we assumed U is universal, it must also be able to clone another distinct state $|\phi\rangle$:

$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle \tag{3.2}$$

We now calculate the inner product of the initial combined states and the final combined states. Quantum mechanics dictates that unitary evolutions preserve inner products. First, we compute the inner product of the **initial** states (before the application of U):

$$\begin{aligned} \langle \Psi_{in} | \Phi_{in} \rangle &= (\langle \psi | \otimes \langle s |)(|\phi\rangle \otimes |s\rangle) \\ &= \langle \psi | \phi \rangle \end{aligned} \tag{3.3}$$

Note that $\langle s|s\rangle = 1$ because the state is normalized. Next, we compute the inner product of the **final** states (after the application of U):

$$\begin{aligned} \langle \Psi_{out} | \Phi_{out} \rangle &= (\langle \psi | \otimes \langle \psi |)(|\phi\rangle \otimes |\phi\rangle) \\ &= (\langle \psi | \phi \rangle)^2 \end{aligned} \tag{3.4}$$

Since U is a unitary operator ($U^\dagger U = I$), it must preserve the inner product between any two states. Therefore, the inner product of the initial states must equal the inner product of the final states:

$$\langle \Psi_{in} | \Phi_{in} \rangle = \langle \Psi_{out} | \Phi_{out} \rangle \tag{3.5}$$

Substituting the results from Eq. (3.3) and Eq. (3.4), we obtain:

$$\langle \psi | \phi \rangle = (\langle \psi | \phi \rangle)^2 \tag{3.6}$$

Let $x = \langle \psi | \phi \rangle$. The algebraic equation $x = x^2$ has only two solutions:

- $x = 1$: This implies $|\psi\rangle = |\phi\rangle$ (the states are identical).
- $x = 0$: This implies $\langle \psi | \phi \rangle = 0$ (the states are orthogonal).

In conclusion, the cloning condition holds **only** if the two states are either identical or orthogonal. It fails for any pair of non-orthogonal states. Consequently, no unitary operator U exists that can perfectly clone an **arbitrary** unknown quantum state. The no-cloning theorem plays a fundamental role in ensuring the security of quantum communication protocols.

3.3 Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) stands out as one of the most developed and practically applicable technologies to emerge from quantum information science. Its primary function is to enable two separated users, commonly referred to as Alice (A) and Bob (B), to generate a shared, private encryption key. The unique advantage here is that security is anchored in the absolute laws of physics, rather than the complexity of mathematical algorithms. Unlike traditional cryptography, where security relies on the assumed computational hardness of certain mathematical problems, QKD provides information-theoretic

security. This means that because of the nature of quantum mechanics, any third party trying to spy on the line will inevitably alter the state of the system, instantly revealing their presence. Functionally, these protocols are built on core quantum concepts, such as the no-cloning theorem, the fact that measuring a system disturbs it, and the non-local connections found in entangled particles. While the theory behind QKD is watertight, implementing it in the real world comes with significant engineering hurdles. Systems must contend with signal loss over distance, imperfect detectors and background environmental noise. Even with these obstacles, however, QKD has been effectively proven using both fiber-optic cables and free-space optical links, establishing itself as a foundational element for future quantum communication networks and repeater systems [25–27].

When looking at how they operate and the hardware they require, QKD protocols generally fall into three primary types: prepare-and-measure, entanglement-based, and measurement-device-independent.

3.3.1 Prepare-and-measure QKD Protocols

Prepare-and-measure QKD protocols are the earliest and conceptually simplest class of QKD schemes. In these protocols, Alice prepares single-qubit quantum states chosen from a predefined set of non-orthogonal states and transmits them to Bob through a quantum channel. Bob performs measurements on the received states using randomly chosen measurement bases. To better understand prepare-and-measure protocols, we will examine the BB84 protocol.

The BB84 protocol, proposed by Bennett and Brassard in 1984 [28], is the first and most widely studied quantum key distribution protocol. It is a prepare-and-measure scheme in which the security of the generated cryptographic key relies on the use of non-orthogonal quantum states and on the fundamental principle that quantum measurements unavoidably disturb the system being measured.

The protocol involves two legitimate parties, Alice (the sender) and Bob (the receiver), who are connected by a quantum channel and an authenticated classical communication channel. The goal of the protocol is to establish a shared secret key while allowing Alice and Bob to detect the presence of a potential eavesdropper, traditionally called Eve.

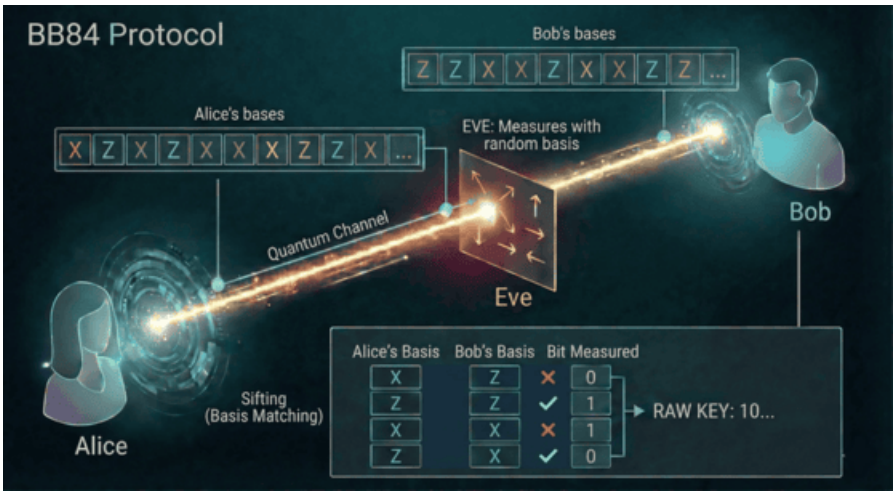

Figure 3.1: Conceptual overview of the BB84 protocol

Step 1: State Preparation

Alice begins by generating two random classical bit strings of equal length:

- A random bit string $\mathbf{b} \in \{0,1\}^n$, which represents the raw key.
- A random basis string $\theta \in \{\mathcal{Z},\mathcal{X}\}^n$, which determines the encoding basis for each bit.

The computational basis $\mathcal{Z} = \{|0\rangle, |1\rangle\}$ and the Hadamard basis $\mathcal{X} = \{|+\rangle, |-\rangle\}$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, are mutually unbiased, meaning that a state prepared in one basis gives completely random measurement outcomes when measured in the other basis, with equal probabilities for all possible results. For each position i, Alice prepares a qubit according to the rule

$$|\psi_i\rangle = \begin{cases} |0\rangle \text{ or } |1\rangle, & \text{if } \theta_i = \mathcal{Z}, \\ |+\rangle \text{ or } |-\rangle, & \text{if } \theta_i = \mathcal{X}, \end{cases}$$

with the specific state determined by the value of b_i. Note that, in photonic implementations, the $\mathcal{Z}$ and $\mathcal{X}$ bases are often referred to as the rectilinear (horizontal/vertical) and diagonal polarization bases, respectively.

Step 2: Quantum Transmission

Alice sends the sequence of prepared qubits to Bob over the quantum channel. Due to the no-cloning theorem, an eavesdropper cannot copy the transmitted qubits without disturbing their states.

Step 3: Measurement

Upon receiving each qubit, Bob independently and randomly chooses a measurement basis $\theta'_i \in \{\mathcal{Z},\mathcal{X}\}$ and performs a projective measurement. Bob records both the measurement outcomes and the bases used.

Step 4: Basis Reconciliation (Sifting)

After the quantum transmission is complete, Alice and Bob communicate over the authenticated classical channel to compare their basis choices. For each position i, they publicly announce θ_i and θ'_i but never disclose the measurement outcomes or encoded bits.

All positions for which $\theta_i \neq \theta'_i$ are discarded. The remaining bits form the *sifted key*. In the absence of noise and eavesdropping, Alice's and Bob's sifted keys are perfectly correlated.

Step 5: Parameter Estimation

To estimate the level of noise and detect potential eavesdropping, Alice and Bob randomly select a subset of the sifted key and publicly compare the corresponding bit values. The fraction of mismatched bits defines the quantum bit error rate (QBER).

If the QBER exceeds a predefined security threshold, the protocol is aborted, as this indicates either excessive noise or the presence of an eavesdropper. Otherwise, the remaining undisclosed bits are retained

for further processing.

Step 6: Error Correction

Due to imperfections in the quantum channel and measurement devices, the remaining bits may still contain discrepancies. Alice and Bob apply a classical error correction protocol over the authenticated classical channel to reconcile their keys while minimizing information leakage to an eavesdropper.

Step 7: Privacy Amplification

Even after error correction, Eve may possess partial information about the key. To eliminate this information, Alice and Bob apply a privacy amplification procedure, typically based on universal hash functions. This process compresses the reconciled key into a shorter final key that is provably secure.

Step 8: Final Key Generation

The output of the privacy amplification stage is a shared secret key known only to Alice and Bob. This key can then be used for cryptographic applications such as one-time pad encryption or symmetric-key cryptography.

3.3.2 Entanglement-based QKD Protocols

Entanglement-based QKD protocols exploit the quantum correlations of entangled states to establish a shared secret key. In these schemes, Alice and Bob share pairs of entangled qubits, either generated by one of the parties or by a third source. By performing local measurements on their respective qubits, Alice and Bob obtain correlated outcomes that can be used to generate a secret key. To better understand entanglement protocols, we will examine the E91 protocol.

The E91 protocol, proposed by Ekert in 1991 [29], is an entanglement-based quantum key distribution scheme in which the security of the generated key is fundamentally tied to the violation of Bell inequalities. In this protocol, the detection of an eavesdropper is achieved by testing whether the observed correlations between Alice's and Bob's measurement outcomes violate a Bell inequality. Any attempt by an adversary (Eve) to gain information necessarily disturbs the entanglement structure, reducing the Bell violation and thereby revealing her presence.

Physical Setup

A source emits pairs of entangled qubits prepared in the singlet state:

$$\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \tag{3.7}$$

where one qubit is sent to Alice and the other to Bob. The source may be controlled by Alice, Bob, or even be untrusted, as the security of the protocol is verified operationally through Bell tests.

Step 1: Random Measurement Basis Selection

For each received qubit, Alice randomly selects one of three measurement bases defined by the azimuthal

angles:

$$\{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\} = \{0^\circ, 45^\circ, 90^\circ\} \tag{3.8}$$

while Bob independently and randomly selects one of his three bases:

$$\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\} = \{45^\circ, 90^\circ, 135^\circ\} \tag{3.9}$$

Each measurement corresponds to a projective measurement of the qubit along the chosen direction, yielding a binary outcome ± 1.

Step 2: Local Measurements

Alice and Bob perform their measurements locally on their respective qubits. Due to quantum entanglement, their outcomes are statistically correlated in a manner that depends on the relative orientation of their measurement settings. Importantly, no classical information is encoded in the particles prior to measurement.

Step 3: Public Announcement of Measurement Settings

After a sufficiently large number of measurement rounds, Alice and Bob publicly announce, over an authenticated classical channel, the measurement settings used in each round. The actual measurement outcomes remain secret at this stage. Based on the announced settings, the data are divided into two subsets:

- **Key Generation Subset:** Rounds where Alice and Bob used compatible settings (specifically $\mathbf{a}_2$ with $\mathbf{b}_1$, and $\mathbf{a}_3$ with $\mathbf{b}_2$).
- **Bell Test Subset:** Rounds with incompatible settings (involving $\mathbf{a}_1, \mathbf{a}_3$ and $\mathbf{b}_1, \mathbf{b}_3$), which are used to test Bell inequalities.

Step 4: Bell Inequality Test

To assess the security of the channel, Alice and Bob publicly reveal the measurement outcomes corresponding strictly to the Bell test subset and compute the correlation coefficients:

$$E(\mathbf{a}_i, \mathbf{b}_j) = P_{++}(\mathbf{a}_i, \mathbf{b}_j) + P_{--}(\mathbf{a}_i, \mathbf{b}_j) - P_{+-}(\mathbf{a}_i, \mathbf{b}_j) - P_{-+}(\mathbf{a}_i, \mathbf{b}_j) \tag{3.10}$$

Using these correlations, they evaluate the Clauser-Horne-Shimony-Holt (CHSH) [30, 31] parameter:

$$S = E(\mathbf{a}_1, \mathbf{b}_1) - E(\mathbf{a}_1, \mathbf{b}_3) + E(\mathbf{a}_3, \mathbf{b}_1) + E(\mathbf{a}_3, \mathbf{b}_3). \tag{3.11}$$

Note that we follow Ekert's original formulation of the CHSH inequality, employing three measurement settings per party and evaluating the Bell parameter on the corresponding subsets of correlations.

Step 5: Eavesdropping Detection

If the inequality

$$|S| \leq 2 \tag{3.12}$$

holds (in practice, finite statistics and experimental noise require a threshold slightly above the classical bound), it indicates that the entanglement of the qubit pairs has been disrupted by an outside intervention or that the system behaves classically. In this case, the protocol is aborted. In contrast, if the experimentally observed value of $|S|$ approaches the quantum mechanical bound $2\sqrt{2}$ [32], Alice and Bob conclude that the shared states are genuinely entangled and that no significant eavesdropping has occurred.

Step 6: Key Generation

From the subset of rounds in which Alice and Bob used identical orientations ($\mathbf{a}_2$ matching $\mathbf{b}_1$, or $\mathbf{a}_3$ matching $\mathbf{b}_2$), quantum mechanics predicts total anticorrelation ($E = -1$) for the singlet state. By locally flipping one party's bits, they obtain identical raw key strings.

Step 7: Classical Post-Processing

As in prepare-and-measure protocols, the raw key is further processed using classical error correction to eliminate discrepancies due to noise, followed by privacy amplification to remove any partial information potentially available to an eavesdropper.

Step 8: Final Key

The output of the protocol is a shared secret key.

3.3.3 Measurement-Device-Independent QKD Protocols

Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) protocols constitute a third major class of QKD schemes, designed to remove all security vulnerabilities associated with the measurement devices. In these protocols, the security of the key does not rely on the trustworthiness of the detectors, which are known to be the most vulnerable components in practical QKD implementations. Instead, all measurements are delegated to an untrusted third party, without compromising security.

The most prominent and widely studied example of this class is the MDI-BB84 protocol, originally proposed by Lo, Curty, and Qi in 2012 [33]. The protocol can be viewed as a hybrid between prepare-and-measure and entanglement-based QKD, and its security can be rigorously proven even if the measurement device is fully controlled by an adversary.

Physical Setup

The MDI-QKD protocol involves three parties: Alice, Bob, and a third node, Charlie. Alice and Bob each possess a trusted source capable of preparing quantum states, while Charlie performs a joint measurement on the incoming signals. Charlie may be dishonest or even identical to the eavesdropper Eve.

No entangled states are distributed initially. Instead, Alice and Bob independently prepare quantum states and send them to Charlie through insecure quantum channels.

Step 1: State Preparation

For each transmission round, Alice and Bob independently and randomly prepare one of the four BB84

states:

$$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}, \tag{3.13}$$

corresponding to a random choice of bit value and basis (computational Z basis or diagonal X basis).

Step 2: Transmission to the Measurement Node

Alice and Bob send their prepared quantum states to Charlie via quantum channels. Since Charlie is untrusted, no assumptions are made about the integrity of the measurement apparatus or detection process.

Step 3: Bell-State Measurement

Upon receiving the quantum states from Alice and Bob, Charlie performs a Bell-state measurement (BSM). Due to experimental limitations, the measurement usually distinguishes only a subset of the four Bell states, such as $|\psi^-\rangle$ and $|\psi^+\rangle$. Charlie then publicly announces whether a successful Bell-state measurement occurred and which Bell state was detected.

Importantly, the announced measurement result does not reveal the individual states or bit values prepared by Alice and Bob.

Step 4: Public Announcement of Bases

After Charlie's announcement, Alice and Bob publicly reveal the measurement bases used in each round, but keep their actual bit values secret. Based on the combination of announced bases and the Bell-state measurement outcome, Alice and Bob can infer whether their bits are correlated or anticorrelated.

Step 5: Sifting and Eavesdropping Detection

Alice and Bob retain only those rounds in which:

- Charlie reports a successful Bell-state measurement
- Alice and Bob used compatible measurement bases.

Rounds that do not satisfy these conditions are discarded.

Step 6: Key Generation

From the retained rounds, Alice and Bob apply appropriate local bit flips, depending on the announced Bell state, in order to obtain identical raw key strings. The correlations between their bits arise effectively from an entanglement-swapping process induced by Charlie's Bell-state measurement.

Step 7: Classical Post-Processing

As in other QKD protocols, the raw key is processed using classical error correction to remove discrepancies due to noise, followed by privacy amplification to eliminate any residual information that may be available to an eavesdropper.

Step 8: Final Key

The final output of the MDI-QKD protocol is a shared secret key whose security is independent of the measurement devices.

3.4 Quantum Teleportation

The concept of teleportation often evokes images from science fiction, where physical objects are dematerialized at one location and instantaneously rematerialized at another. In the context of quantum information theory, however, **Quantum Teleportation** refers to a distinct and strictly defined protocol: the transfer of an unknown quantum state $|\psi\rangle$ from a sender to a receiver without the physical transmission of the particle itself.

Proposed by Bennett *et al.* in 1993 [34], quantum teleportation relies on two fundamental resources:

1. A shared entangled pair (typically a Bell state, such as $|\Phi^+\rangle$) distributed beforehand between the sender and the receiver.

2. A classical communication channel to transmit two classical bits of information.

It is crucial to emphasize that quantum teleportation involves the transfer of **quantum information**, not matter. The physical carrier of the state at the sender's side is not moved to the receiver. Its quantum state is effectively destroyed and reconstructed on a particle already in the receiver's possession. Furthermore, this protocol strictly adheres to the fundamental laws of physics:

- **No-Cloning Theorem:** Teleportation does not create a copy of the quantum state. The original state $|\psi\rangle$ at the sender's side is necessarily destroyed (via measurement) during the process, ensuring that the state exists only at one location at a time.

- **No Superluminal Communication:** Although quantum correlations are established instantaneously upon measurement, the receiver cannot reconstruct the state $|\psi\rangle$ until the classical measurement outcomes are received. Since classical information is bound by the speed of light, quantum teleportation cannot be used to transmit information faster than light.

In the following analysis, we will examine the detailed mathematical formulation and step-by-step implementation of the protocol for two communicating parties Alice and Bob:

Step 1: Entangled Qubit Pair Generation

An entangled qubit pair between Alice and Bob is generated.

i Alice's qubit $|q_A\rangle$ and Bob's qubit $|q_B\rangle$ are initialized to state $|0\rangle$:

$$|\psi_0\rangle = |q_A\rangle \otimes |q_B\rangle = |00\rangle_{AB} \tag{3.14}$$

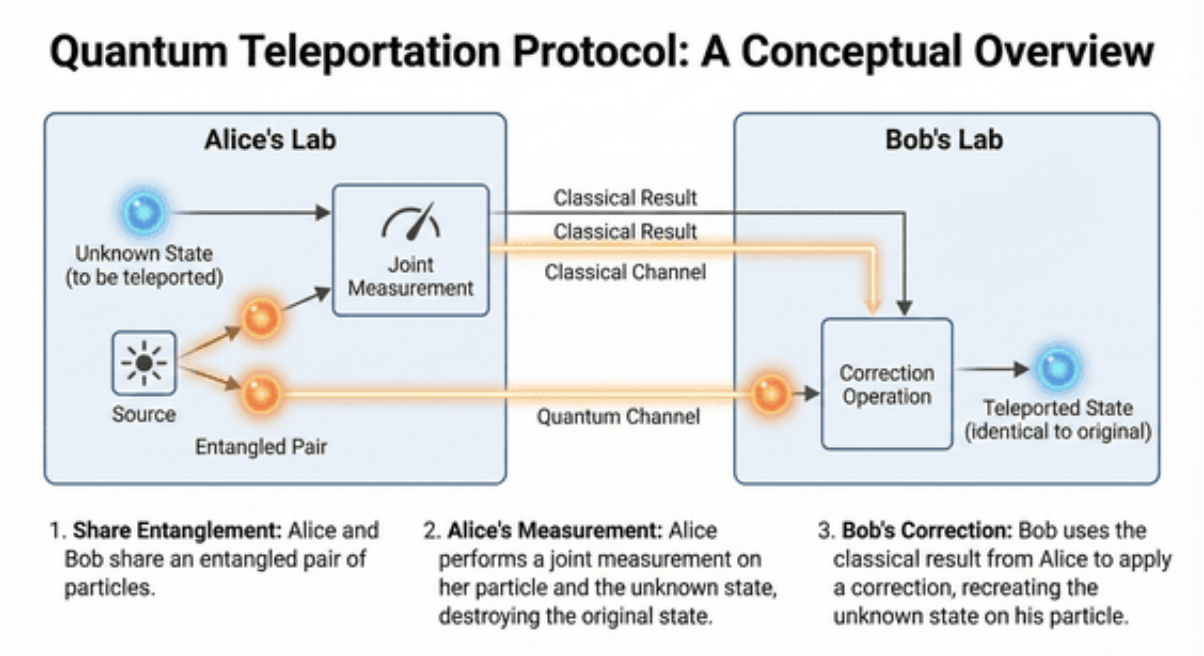

Figure 3.2: Conceptual overview of the quantum teleportation protocol

ii A Hadamard gate is applied to $|q_A\rangle$:

$$|\psi_1\rangle = (H \otimes I)\,|00\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A \otimes |0\rangle_B = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |10\rangle_{AB}) \tag{3.15}$$

iii A CNOT gate is applied with q_A as the control qubit and q_B as the target qubit:

$$\begin{aligned} |\psi_2\rangle &= CNOT\left[\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |10\rangle_{AB})\right] \\ &= \frac{1}{\sqrt{2}}(CNOT\,|00\rangle_{AB} + CNOT\,|10\rangle_{AB}) \\ &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \left|\Phi^+\right\rangle_{AB} \end{aligned} \tag{3.16}$$

Note that $|\Phi^+\rangle$ is one of the four maximally entangled Bell states.

The schematic representation of the entangled (Bell) state generation is the following:

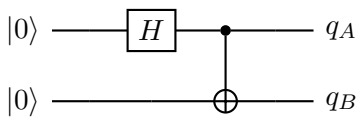

Figure 3.3: Circuit for generating Bell state $|\Phi^+\rangle$.

Suppose now that Alice wishes to teleport an unknown single-qubit state $|q\rangle$. The state of $|q\rangle$ can be expressed as a general superposition state:

$$|q\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \alpha, \beta \in \mathbb{C} \tag{3.17}$$

The state of the 3-qubit system is now:

$$\begin{aligned}|\psi_3\rangle &= (\alpha|0\rangle + \beta|1\rangle)_q \otimes \left|\Phi^+\right\rangle_{AB} \\ &= \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)_q(|00\rangle_{AB} + |11\rangle_{AB}) \\ &= \frac{1}{\sqrt{2}}(\alpha|000\rangle_{qAB} + \alpha|011\rangle_{qAB} + \beta|100\rangle_{qAB} + \beta|111\rangle_{qAB})\end{aligned} \tag{3.18}$$

Step 2: Bell-state Measurement

A Bell-state measurement is performed on $|q\rangle$ and $|q_A\rangle$. A Bell-state Measurement (BSM) is a joint quantum measurement performed on a system of two qubits, which projects their combined state onto one of the four maximally entangled Bell states ($|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle$). Unlike standard local measurements that determine the state of individual qubits, a BSM reveals the correlation between the two particles without disclosing their individual properties.

i A CNOT gate is applied with $|q\rangle$ as the control qubit and $|q_A\rangle$ as the target qubit:

$$\begin{aligned}|\psi_4\rangle &= \frac{1}{\sqrt{2}}CNOT_{qA}(\alpha|000\rangle_{qAB} + \alpha|011\rangle_{qAB} + \beta|100\rangle_{qAB} + \beta|111\rangle_{qAB}) \\ &= \frac{1}{\sqrt{2}}(\alpha CNOT|00\rangle_{qA}|0\rangle_B + \alpha CNOT|01\rangle_{qA}|1\rangle_B + \beta CNOT|10\rangle_{qA}|0\rangle_B + \beta CNOT|11\rangle_{qA}|1\rangle_B) \\ &= \frac{1}{\sqrt{2}}(\alpha|000\rangle_{qAB} + \alpha|011\rangle_{qAB} + \beta|110\rangle_{qAB} + \beta|101\rangle_{qAB})\end{aligned} \tag{3.19}$$

ii A Hadamard gate is applied to $|q\rangle$:

$$\begin{aligned}|\psi_5\rangle &= \frac{1}{\sqrt{2}}(\alpha H|0\rangle_q|00\rangle_{AB} + \alpha H|0\rangle_q|11\rangle_{AB} + \beta H|1\rangle_q|10\rangle_{AB} + \beta H|1\rangle_q|01\rangle_{AB}) \\ &= \frac{1}{2}\big(\alpha|000\rangle_{qAB} + \alpha|100\rangle_{qAB} + \alpha|011\rangle_{qAB} + \alpha|111\rangle_{qAB} \\ &\quad + \beta|010\rangle_{qAB} - \beta|110\rangle_{qAB} + \beta|001\rangle_{qAB} - \beta|101\rangle_{qAB}\big)\end{aligned} \tag{3.20}$$

The equation can be factorized with respect to $|q\rangle$ and $|q_A\rangle$:

$$\begin{aligned}|\psi_5\rangle = \frac{1}{2}\big[&|00\rangle_{qA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) \\ &+ |01\rangle_{qA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) \\ &+ |10\rangle_{qA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) \\ &+ |11\rangle_{qA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)\big]\end{aligned} \tag{3.21}$$

iii Alice performs a measurement on $|q\rangle$ and $|q_A\rangle$ and informs Bob of the outcome via a classical channel.

The schematic representation of the BSM is the following:

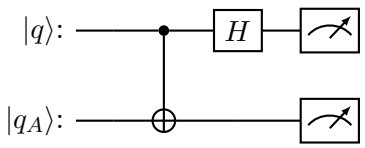

Figure 3.4: Circuit diagram of the BSM.

Step 3: Correction

There are four equally probable measurement outcomes of $|q\rangle$ and $|q_A\rangle$. It follows that Bob's qubit $|q_B\rangle$ is projected onto a corresponding conditional state, based on the measurement outcome. Bob applies the appropriate correction gates on $|q_B\rangle$ to obtain the desired state as shown in eq. (3.17). The following gates are used for the correction:

$$\begin{aligned} &Identity : I|0\rangle = |0\rangle, I|1\rangle = |1\rangle \\ &Pauli - X(bit - flip) : X|0\rangle = |1\rangle, X|1\rangle = |0\rangle \\ &Pauli - Z(phase - flip) : Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle \end{aligned} \tag{3.22}$$

Suppose that the measurement on $|q\rangle$ and $|q_A\rangle$ yielded an outcome of $|11\rangle$. It is evident from eq. (3.21) that $|q_B\rangle$ is projected onto the state:

$$|q_B\rangle_0 = \alpha|1\rangle - \beta|0\rangle \tag{3.23}$$

First, Bob applies a Pauli-X gate:

$$|q_B\rangle_1 = X(\alpha|1\rangle - \beta|0\rangle) = \alpha X|1\rangle - \beta X|0\rangle = \alpha|0\rangle - \beta|1\rangle \tag{3.24}$$

Bob now applies a Pauli-Z gate:

$$|q_B\rangle_2 = Z(\alpha|0\rangle - \beta|1\rangle) = \alpha Z|0\rangle - \beta Z|1\rangle = -\alpha|0\rangle - \beta|1\rangle = -1(\alpha|0\rangle + \beta|1\rangle) \tag{3.25}$$

The global phase factor -1 can be ignored, as it has no observable physical consequence. Thus, the final post-correction state of $|q_B\rangle$ is:

$$|q_B\rangle_3 = \alpha|0\rangle + \beta|1\rangle \tag{3.26}$$

Table 3.1: Measurement outcome and appropriate correction

Measurement Outcome	Correction
$\|00\rangle_{qA}$	Identity gate I
$\|01\rangle_{qA}$	Pauli-X gate
$\|10\rangle_{qA}$	Pauli-Z gate
$\|11\rangle_{qA}$	Pauli-X gate followed by Pauli-Z gate

After the application of the correction gates, the target state has been successfully teleported and the quantum teleportation protocol is complete.

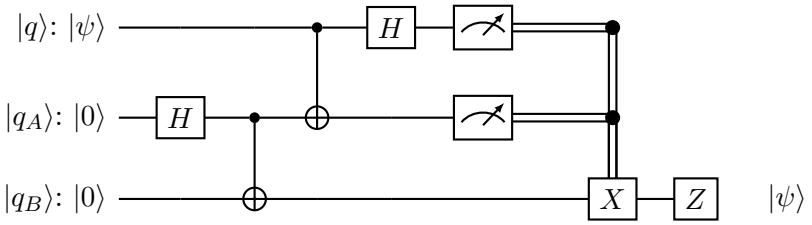

Figure 3.5: Quantum teleportation circuit

This protocol highlights the fundamental role of entanglement and classical communication in quantum information processing and serves as a building block for more advanced quantum communication schemes.

3.5 Entanglement Swapping Protocol

Entanglement swapping is a fundamental protocol in quantum information science that enables two quantum systems, which have never interacted and may be spatially separated, to become entangled through the use of intermediate measurements. First proposed by Żukowski *et al.* in 1993 [35], entanglement swapping extends the concept of quantum entanglement beyond direct physical interaction and plays a central role in quantum repeaters, quantum networks, and long-distance quantum communication.

The swapping protocol relies on two fundamental resources:

1. An intermediate party that shares an entangled qubit pair with each of the two communicating parties.
2. A classical communication channel to transmit two classical bits of information.

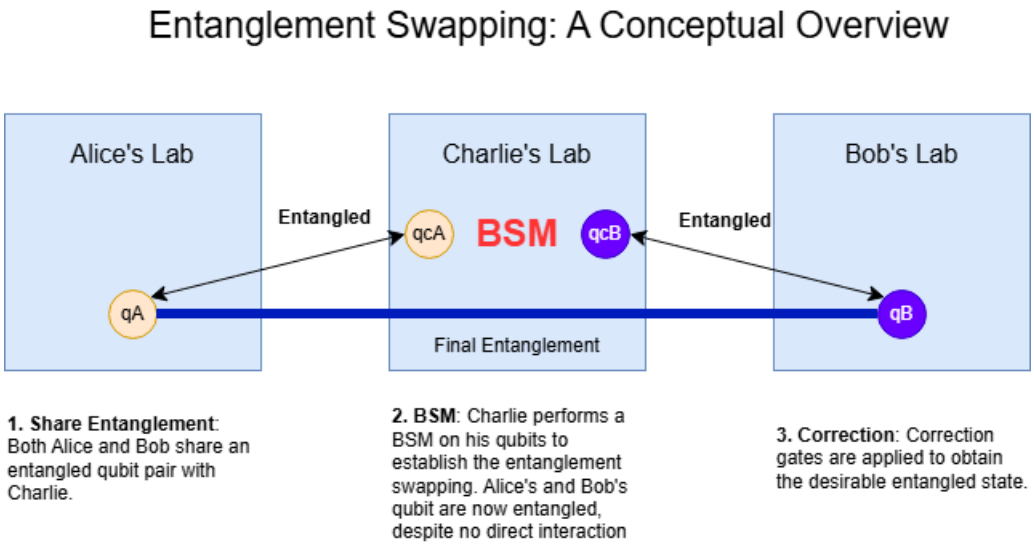

Figure 3.6: Conceptual overview of the entanglement swapping protocol

In the following analysis, we will examine the detailed mathematical formulation and step-by-step implementation of the protocol for two communicating parties Alice and Bob and a third intermediate party

Charlie:

Step 1: Entangled Qubit Pairs Generation

Two independent entangled qubit pairs are generated: one shared between Alice and Charlie, and one shared between Bob and Charlie. Alice's qubit $|q_A\rangle$ is entangled with Charlie's qubit $|q_C\rangle$ and Bob's qubit $|q_B\rangle$ is entangled with Charlie's qubit $|q_D\rangle$.
The starting state of the system is the following:

$$\begin{aligned} |\psi_0\rangle &= \left|\Phi^+\right\rangle_{AC} \otimes \left|\Phi^+\right\rangle_{BD} \\ &= \frac{1}{2}(|0000\rangle_{ACBD} + |0011\rangle_{ACBD} + |1100\rangle_{ACBD} + |1111\rangle_{ACBD}) \end{aligned} \tag{3.27}$$

Note that at this stage, qubits $|q_A\rangle$ and $|q_B\rangle$ are not entangled with each other.
We can rewrite the state, expressed as the sum of tensor products of qubits $|q_A\rangle$, $|q_B\rangle$ and qubits $|q_C\rangle$, $|q_D\rangle$:

$$|\psi_0\rangle = \frac{1}{2}\left(|00\rangle_{AB}|00\rangle_{CD} + |01\rangle_{AB}|01\rangle_{CD} + |10\rangle_{AB}|10\rangle_{CD} + |11\rangle_{AB}|11\rangle_{CD}\right) \tag{3.28}$$

Step 2: Bell-state Measurement

A Bell-state measurement is performed by Charlie on his qubits.

i) A CNOT gate is applied with $|q_C\rangle$ as the control qubit and $|q_D\rangle$ as the target qubit:

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{2}\big(|00\rangle_{AB}\,CNOT\,|00\rangle_{CD} + |01\rangle_{AB}\,CNOT\,|01\rangle_{CD} \\ &\quad + |10\rangle_{AB}\,CNOT\,|10\rangle_{CD} + |11\rangle_{AB}\,CNOT\,|11\rangle_{CD}\big) \\ &= \frac{1}{2}\left(|00\rangle_{AB}|00\rangle_{CD} + |01\rangle_{AB}|01\rangle_{CD} + |10\rangle_{AB}|11\rangle_{CD} + |11\rangle_{AB}|10\rangle_{CD}\right) \end{aligned} \tag{3.29}$$

ii) A Hadamard gate is applied to $|q_C\rangle$:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}\big(|00\rangle_{AB}\,H\,|0\rangle_C\,|0\rangle_D + |01\rangle_{AB}\,H\,|0\rangle_C\,|1\rangle_D \\ &\quad + |10\rangle_{AB}\,H\,|1\rangle_C\,|1\rangle_D + |11\rangle_{AB}\,H\,|1\rangle_C\,|0\rangle_D\big) \\ &= \frac{1}{2\sqrt{2}}\big[|00\rangle_{AB}\,(|0\rangle_C + |1\rangle_C)\,|0\rangle_D + |01\rangle_{AB}\,(|0\rangle_C + |1\rangle_C)\,|1\rangle_D \\ &\quad + |10\rangle_{AB}\,(|0\rangle_C - |1\rangle_C)\,|1\rangle_D + |11\rangle_{AB}\,(|0\rangle_C - |1\rangle_C)\,|0\rangle_D\big] \\ &= \frac{1}{2\sqrt{2}}\big[|00\rangle_{AB}\,(|00\rangle_{CD} + |10\rangle_{CD}) + |01\rangle_{AB}\,(|01\rangle_{CD} + |11\rangle_{CD}) \\ &\quad + |10\rangle_{AB}\,(|01\rangle_{CD} - |11\rangle_{CD}) + |11\rangle_{AB}\,(|00\rangle_{CD} - |10\rangle_{CD})\big] \end{aligned} \tag{3.30}$$

The expression can be factorized with respect to $|q_C q_D\rangle$:

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2\sqrt{2}}\big[&|00\rangle_{CD}\left(|00\rangle_{AB} + |11\rangle_{AB}\right) + |01\rangle_{CD}\left(|01\rangle_{AB} + |10\rangle_{AB}\right) \\ &+ |10\rangle_{CD}\left(|00\rangle_{AB} - |11\rangle_{AB}\right) + |11\rangle_{CD}\left(|01\rangle_{AB} - |10\rangle_{AB}\right)\big] \\ = \frac{1}{2}(&|00\rangle_{CD}\left|\Phi^+\right\rangle_{AB} + |01\rangle_{CD}\left|\Psi^+\right\rangle_{AB} + |10\rangle_{CD}\left|\Phi^-\right\rangle_{AB} + |11\rangle_{CD}\left|\Psi^-\right\rangle_{AB})\end{aligned} \tag{3.31}$$

It follows that each of the four Bell-state measurement outcomes occurs with equal probability and projects qubits $|q_A\rangle$ and $|q_B\rangle$ onto a corresponding Bell state:

Table 3.2: Measurement outcome and respective Bell state

Measurement Outcome ($\|q_C\rangle$, $\|q_D\rangle$)	Bell state ($\|q_A\rangle$, $\|q_B\rangle$)
$\|00\rangle$	$\|\Phi^+\rangle$
$\|01\rangle$	$\|\Psi^+\rangle$
$\|10\rangle$	$\|\Phi^-\rangle$
$\|11\rangle$	$\|\Psi^-\rangle$

Step 3: Correction

Charlie informs Alice and Bob via a classical channel of the measurement outcome. At this point, the entanglement swapping has been completed. However, the specific Bell state can be any one of the four with equal probability. For future use of the entangled qubit pair $|q_A\rangle, |q_B\rangle$, it is often desirable for Alice and Bob to prepare a specific Bell state. Thus, the protocol is completed once the appropriate local correction gates are applied and the desired Bell state is obtained.

Suppose that the desired Bell state is $|\Phi^+\rangle_{AB}$ and that the measurement yielded an outcome of $|11\rangle_{CD}$. That means that qubits $|q_A\rangle$, $|q_B\rangle$ are currently in Bell state $|\Psi^-\rangle$:

$$|q_A q_B\rangle_0 = \left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}) \tag{3.32}$$

First, Alice applies a Pauli-X gate:

$$\begin{aligned}|q_A q_B\rangle_1 &= \frac{1}{\sqrt{2}}(X|0\rangle_A|1\rangle_B - X|1\rangle_A|0\rangle_B) \\ &= \frac{1}{\sqrt{2}}(|11\rangle_{AB} - |00\rangle_{AB})\end{aligned} \tag{3.33}$$

Alice now applies a Pauli-Z gate:

$$\begin{aligned}|q_A q_B\rangle_2 &= \frac{1}{\sqrt{2}}(Z|1\rangle_A|1\rangle_B - Z|0\rangle_A|0\rangle_B) \\ &= \frac{1}{\sqrt{2}}(-|11\rangle_{AB} - |00\rangle_{AB}) = \frac{-1}{\sqrt{2}}\left[(|11\rangle_{AB} + |00\rangle_{AB})\right]\end{aligned} \tag{3.34}$$

The global phase factor -1 can be ignored, as it has no observable physical consequence. Thus, the final

post-correction Bell state of $|q_A\rangle$ and $|q_B\rangle$ is:

$$|q_A q_B\rangle_3 = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \left|\Phi^+\right\rangle_{AB} \tag{3.35}$$

Table 3.3: Measurement outcome and corresponding local correction (desired state $|\Phi^+\rangle$)

Measurement Outcome ($\|q_C\rangle$, $\|q_D\rangle$)	Correction (on $\|q_A\rangle$)
$\|00\rangle$	Identity gate I
$\|01\rangle$	Pauli-X gate
$\|10\rangle$	Pauli-Z gate
$\|11\rangle$	Pauli-X gate followed by Pauli-Z gate

After the application of the correction gates, the desired Bell state has been obtained and the entanglement swapping protocol is complete.

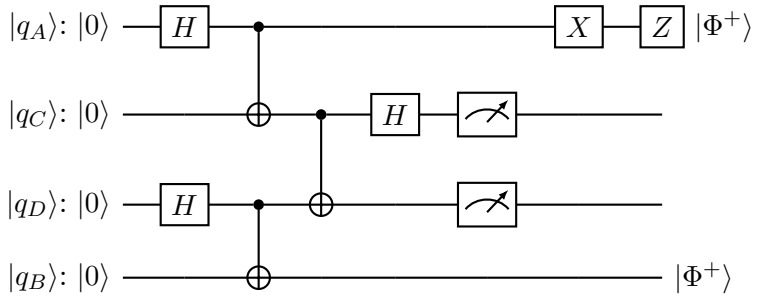

Figure 3.7: Entanglement swapping circuit

Entanglement swapping reveals a profound aspect of quantum mechanics: entanglement can be viewed as a resource that can be redistributed and extended across a network. In practical terms, this protocol forms the backbone of **quantum repeater architectures** [11,36,37] , which are essential for overcoming losses and decoherence in long-distance quantum communication. By connecting multiple entanglement swapping operations, entanglement can be established over large distances, enabling the realization of large-scale communication networks.

Chapter 4: Qiskit and IBM Quantum: A Practical Introduction

4.1 Practical Quantum Programming with Qiskit and IBM Quantum

While quantum information theory provides the conceptual foundation for quantum computation and communication, practical experimentation requires concrete tools for constructing, simulating, and executing quantum circuits. In this context, Qiskit and the IBM Quantum platform provide an end-to-end environment that bridges abstract quantum algorithms with real quantum hardware. This section presents a tutorial-style introduction to Qiskit and the IBM Quantum Composer, focusing on circuit construction, simulation, and measurement.

4.1.1 Qiskit SDK

Qiskit (Quantum Information Science Kit) is an open-source [38] software development kit (SDK) designed to enable the full quantum computing workflow, from algorithm design to execution on real quantum hardware. Written primarily in Python, Qiskit provides an abstraction layer that allows users to construct quantum circuits without requiring direct interaction with the underlying physical implementation.

4.1.2 The Quantum Circuit Model in Qiskit

Qiskit adopts the quantum circuit model as its fundamental computational paradigm. A quantum circuit consists of a finite number of qubits, initialized in a reference state (typically $|0\rangle^{\otimes n}$), upon which quantum gates are applied sequentially. These gates correspond to unitary operations acting on one or more qubits, followed optionally by measurements that map quantum states to classical outcomes. A register of n qubits is represented as $|q_n, q_{n-1}, \ldots, q_1, q_0\rangle$.

In Qiskit, quantum circuits are represented by the `QuantumCircuit` object. Each circuit explicitly defines:

- the number of quantum registers (qubits),
- the number of classical registers (bits),
- the sequence of quantum gates,
- the placement of measurements.

This explicit separation between quantum and classical registers reflects the hybrid nature of quantum computation, where classical post-processing plays a crucial role.

4.1.3 Constructing Quantum Circuits Programmatically

The construction of a quantum circuit in Qiskit begins by specifying the number of qubits and classical bits. Quantum gates are then applied to the circuit using high-level function calls that correspond directly to standard quantum gates.

Single-qubit gates such as the Hadamard (H), Pauli (X, Y, Z), and phase gates are used to create superposition and control relative phases. Multi-qubit gates, most notably the controlled-NOT (CNOT) gate, enable the creation of entangled states. For example, the preparation of a Bell state follows a simple and physically transparent sequence: a Hadamard gate creates a superposition on the first qubit, and a CNOT gate entangles it with the second qubit.

In the following, we construct a simple quantum circuit for the preparation of a Bell state step-by-step:

Step 1: Importing the required libraries

The first step consists of importing the `QuantumCircuit` class from the Qiskit framework. The `QuantumCircuit` object provides the core functionality required for defining quantum registers, applying quantum gates, and managing measurements.

Step 2: Circuit creation

A quantum circuit, denoted by *qc*, is initialized with two qubits using the command *qc = QuantumCircuit(2)*. At this stage, the circuit implicitly assumes that all qubits are initialized in the computational basis state $|0\rangle$.

Step 3: Applying quantum gates

To apply a quantum gate to the circuit, three elements must be specified:

- the quantum circuit object (in this case *qc*),
- the desired quantum gate (for example, `h` for the Hadamard gate),
- the index or indices of the qubit(s) on which the gate acts.

Step 4: Visualization

Qiskit provides built-in tools for visualizing quantum circuits in schematic form. By invoking the `draw` method, the complete structure of the circuit can be rendered graphically, allowing direct inspection of gate ordering and qubit connectivity.

Listing 1 illustrates the programmatic creation of the circuit, while Figure 4.1 shows the corresponding quantum circuit diagram.

```
from qiskit import QuantumCircuit

# Create a Quantum Circuit acting on a quantum register of 2 qubits
qc = QuantumCircuit(2)
```

```
5
6  # Apply a Hadamard gate to qubit 0
7  qc.h(0)
8
9  # Apply a CX (CNOT) gate to control qubit 0 and target qubit 1
10 qc.cx(0, 1)
11
12 # Draw the circuit
13 print(qc.draw())
```

Listing 1: Simple circuit creation using Qiskit

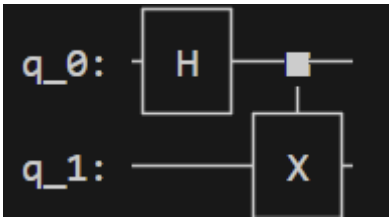

Figure 4.1: Circuit's schematic

4.1.4 Measurements and Classical Readout

Measurement constitutes a fundamental departure from unitary quantum evolution. While quantum gates correspond to deterministic unitary transformations, measurement introduces an irreversible and probabilistic process. In Qiskit, measurements are explicitly appended to a quantum circuit and map quantum states onto classical bits, producing classical outcomes that can be processed using standard computational tools.

From a physical point of view, measuring a qubit corresponds to projecting its quantum state onto a fixed measurement basis, typically the computational basis $\{|0\rangle, |1\rangle\}$. The outcome of this projection is based on the squared magnitudes of the state amplitudes.

In this subsection, we extend the Bell state preparation circuit introduced previously by including a single measurement step and explain how the simulator determines the measurement outcome based on the underlying quantum probabilities.

Step 1: Adding classical registers

To store measurement outcomes, Qiskit requires the explicit definition of classical bits. These classical registers are used to record the result of measuring a quantum qubit. Each measurement operation establishes a mapping between a specific qubit and a classical bit.

For a two-qubit Bell state circuit, two classical bits are introduced to record the outcomes of the measurements performed on each qubit.

Step 2: Appending measurement operations

Measurements are added to the circuit using the `measure` command, which specifies both the quantum

qubit being measured and the classical bit in which the result is stored. Once a qubit is measured, its quantum state is irreversibly collapsed and cannot be used coherently in subsequent gate operations within the same circuit.

At the abstract circuit level, Qiskit enforces this separation between quantum evolution and classical readout, reflecting the physical irreversibility of quantum measurement.

Step 3: How measurement outcomes are determined

Consider a single qubit prepared in the quantum state

$$|\psi\rangle = \sqrt{0.9}\,|0\rangle + \sqrt{0.1}\,|1\rangle\,. \tag{4.1}$$

Measuring this qubit in the computational basis yields the outcome $|0\rangle$ with probability 0.9 and $|1\rangle$ with probability 0.1.

It is common to employ a simulator for the measurements such as **Qiskit Aer**. Qiskit Aer is a high-performance simulator framework for quantum circuits that provides several backends for realistic noise modeling and classical verification. It allows researchers to execute and test complex quantum algorithms locally before deploying them on actual quantum hardware.

When using such a simulator, the measurement process is implemented through probabilistic sampling. Internally, the simulator generates a random number uniformly distributed in the interval $[0, 1)$. If the generated number lies in the interval corresponding to the cumulative probability of $|0\rangle$, the measurement outcome is recorded as 0. Otherwise, the outcome is recorded as 1.

In this example, random values in the range $[0, 0.9)$ lead to the outcome 0, while values in the range $[0.9, 1)$ lead to the outcome 1. This procedure ensures that repeated executions of the same circuit reproduce the correct probability distribution dictated by quantum mechanics.

Step 4: Single-shot measurement in simulation In the present context, the circuit is executed only once, corresponding to a single-shot measurement. As a result, the simulator returns a single classical bitstring rather than a statistical distribution. Although no physical collapse occurs within the simulator, the returned result faithfully represents the outcome of an individual quantum measurement experiment.

For the Bell state prepared in the previous subsection, a single-shot measurement yields either the outcome `00` or `11`. The absence of outcomes `01` and `10` reflects the perfect quantum correlations characteristic of a maximally entangled state, even at the level of individual measurement events.

Step 5: Interpretation of the measurement result The classical bitstring obtained from the measurement represents one realization of the underlying quantum probability distribution. While a single measurement outcome provides limited information, it constitutes the fundamental building block of all experimental quantum data. In subsequent sections, repeated measurements will be used to reconstruct probability distributions and quantitatively analyze quantum correlations.

4.1.5 Repeated Executions and Measurement Statistics (Shots)

A single execution of a quantum circuit yields only one possible measurement outcome, reflecting the inherently probabilistic nature of quantum measurement. While such a single-shot result is physically meaningful, it provides no information about the underlying probability distribution of the quantum state. To extract statistically significant information, quantum circuits must be executed repeatedly.

In Qiskit, repeated executions of the same quantum circuit are controlled by the parameter *shots*. Each shot corresponds to an independent realization of the quantum experiment, including state preparation, quantum evolution, and measurement.

Step 1: Motivation for repeated measurements

Measurement outcomes are governed by probability amplitudes. For a quantum state

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{4.2}$$

the probabilities of measuring $|0\rangle$ and $|1\rangle$ are given by $|\alpha|^2$ and $|\beta|^2$, respectively. However, these probabilities cannot be inferred from a single measurement. Only by performing a large number of measurements can the empirical frequencies converge to the theoretical probabilities.

This principle mirrors classical statistical experiments, where repeated trials are required to estimate unknown probability distributions.

Step 2: The concept of shots in Qiskit

In Qiskit, the `shots` parameter specifies how many times a quantum circuit is executed on a given backend. Each execution produces one classical outcome, and the full set of outcomes is collected into a histogram representing the empirical probability distribution.

Importantly, each shot is statistically independent and corresponds to a fresh preparation of the initial quantum state. This ensures that the measurement statistics accurately reflect the quantum state prior to measurement.

Step 3: Executing a circuit with multiple shots

The following example extends the Bell state circuit introduced previously by executing it multiple times using the `AerSimulator` backend:

```
from qiskit import QuantumCircuit
from qiskit_aer import AerSimulator

# Create a Quantum Circuit acting on a quantum register of 2 qubits and a classical
    register of 2 bits
qc = QuantumCircuit(2,2)

# Apply a Hadamard gate to qubit 0
qc.h(0)

```

```
# Apply a CX (CNOT) gate to control qubit 0 and target qubit 1
qc.cx(0, 1)

# Measure the qubits and store the classical bit value on the classical register
qc.measure(0, 0)
qc.measure(1, 1)

# Use the AerSimulator
simulator = AerSimulator()

# Execute the circuit with 1024 shots
job = simulator.run(qc, shots=1024)

# Get results
result = job.result()
counts = result.get_counts(qc)
print(counts)
```

Listing 2: Repeated measurements using AerSimulator

Step 4: Interpretation of measurement statistics

For the Bell state

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{4.3}$$

quantum theory predicts that the outcomes `00` and `11` should occur with equal probability, while all other outcomes should be absent. This is validated by the outcome of the qiskit program, which yielded 506 counts for state '11' and 518 counts for state '00'.

As the number of shots increases, the relative frequencies of these outcomes converge toward their theoretical values of approximately 50%. Deviations from exact equality are expected for finite shot numbers and arise from statistical fluctuations.

4.1.6 Execution on IBM Quantum Hardware

Once a circuit has been validated through simulation, it can be executed on real quantum processors provided by IBM Quantum. This process involves selecting a backend, transpiling the circuit to match the device's native gate set and connectivity constraints, and submitting the job via the cloud.

The transpilation stage is particularly important, as it translates logical circuits into physically realizable operations. Device-specific constraints such as limited qubit connectivity and varying gate fidelities directly influence circuit depth and overall performance.

Execution results obtained from real hardware reflect the presence of noise and decoherence, offering critical insight into the limitations of current devices.

4.1.7 The IBM Quantum Composer: Graphical Circuit Design

In addition to programmatic circuit construction, IBM Quantum provides the **Quantum Composer** [39], a graphical interface for designing quantum circuits. The Composer allows users to build circuits visually by dragging and placing quantum gates on qubit wires. The Composer's functions and capabilities are presented in the following subsection.

Quantum circuit generation

The number of qubits and classical bits can be specified by the user, and all standard quantum gates are available.

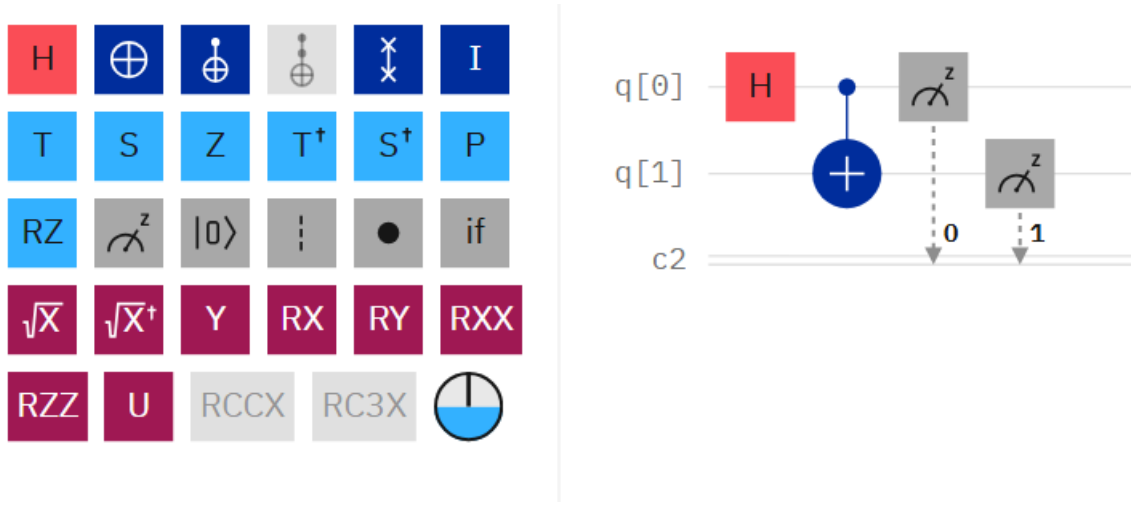

Figure 4.2: Circuit creation on IBM Quantum Composer

Measurement Probabilities

The composer simulates repeated measurements (1024 shots) and presents the probabilities for all qubits measured.

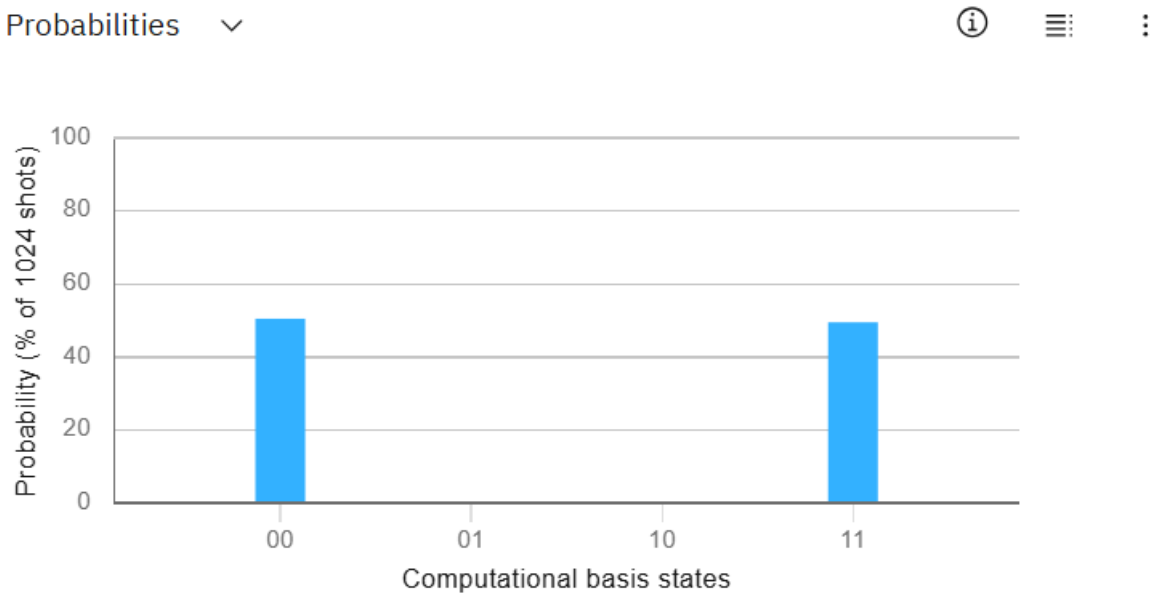

Figure 4.3: Measurement simulation

Qiskit code generation

The circuit is automatically transcribed into Qiskit code.

```
1   from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit
2   from numpy import pi
3
4   qreg_q = QuantumRegister(2, 'q')
5   creg_c = ClassicalRegister(2, 'c')
6   circuit = QuantumCircuit(qreg_q, creg_c)
7
8   circuit.h(qreg_q[0])
9   circuit.cx(qreg_q[0], qreg_q[1])
10  circuit.measure(qreg_q[0], creg_c[0])
11  circuit.measure(qreg_q[1], creg_c[1])
```

Figure 4.4: Auto-generated Qiskit code

Using quantum hardware

The user can run the circuit on real quantum hardware provided by IBM, by clicking *Set up and run* from the composer. The user must first configure some settings, including the number of shots.

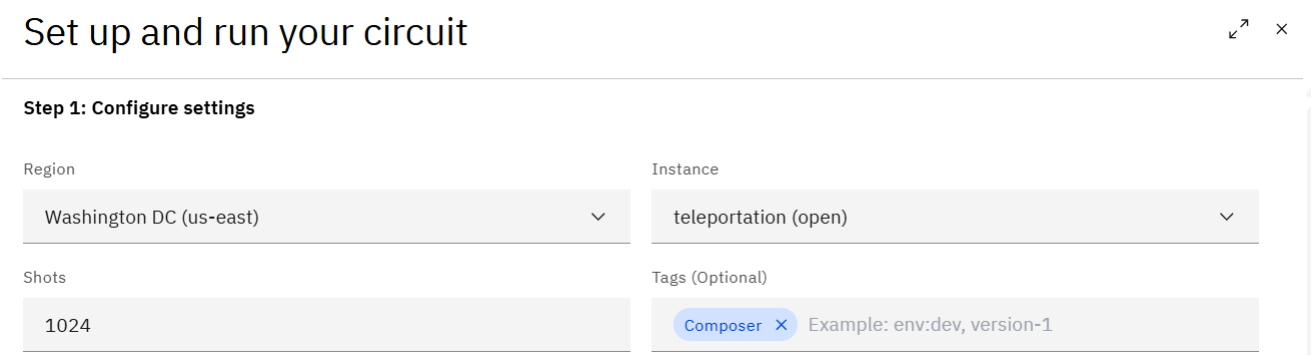

Figure 4.5: Settings

The user must then select a Quantum Processing Unit (QPU) on which the circuit is going to be executed.

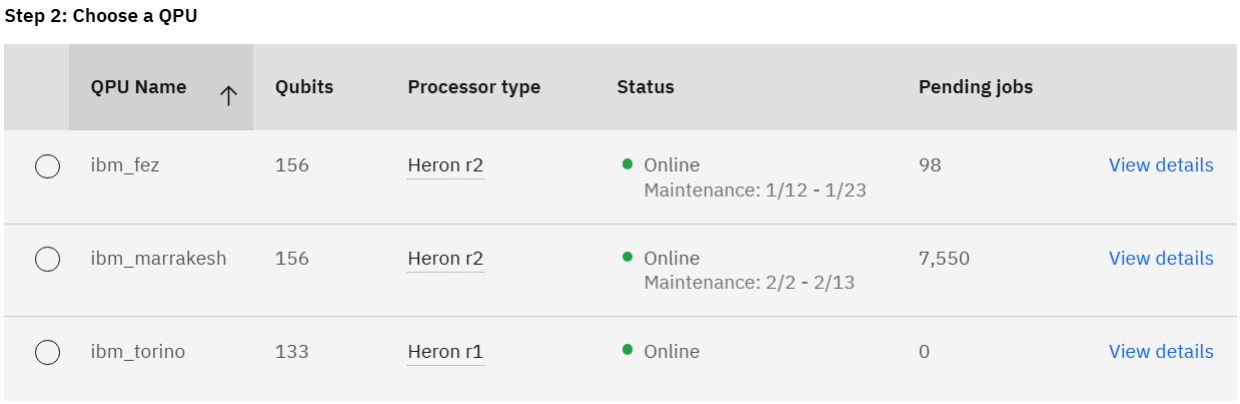

Figure 4.6: QPU selection

The measurement results of the QPU used are presented as a histogram.

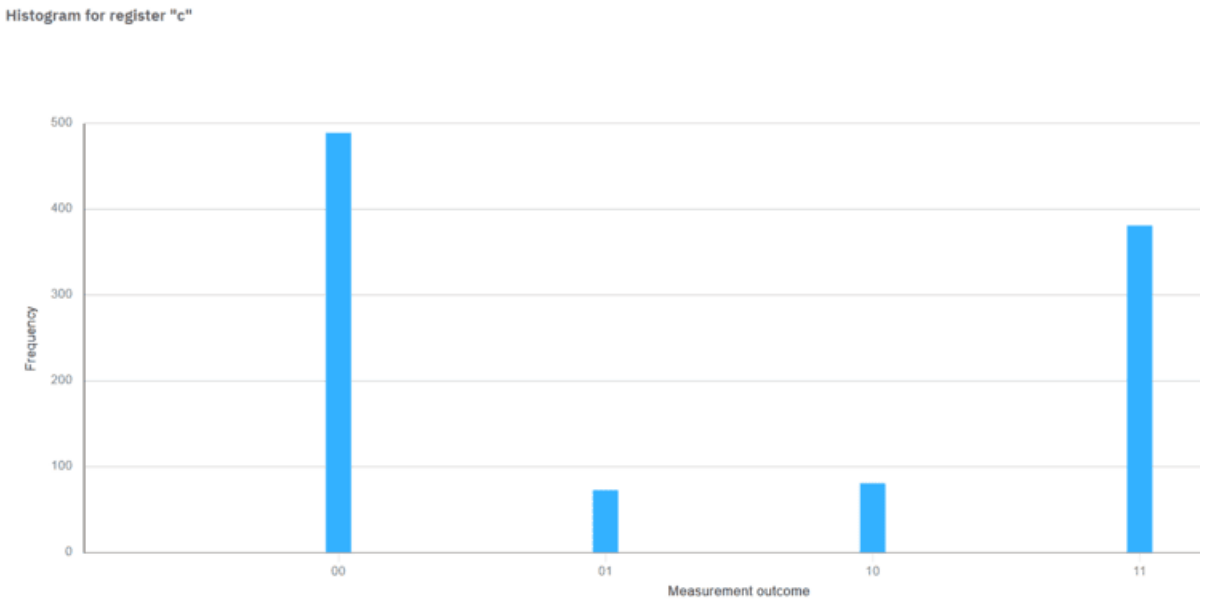

Figure 4.7: Measurement results (1024 shots)

Note that a few measurements yielded results other than `00` and `11`, due to the inherent noise in real quantum hardware.

In summary, the IBM Quantum Composer provides a user-friendly graphical interface that bridges visual circuit design with Qiskit programmatic representation, enabling both simulation and execution on real quantum hardware.

4.1.8 Relevance to Quantum Communication Protocols

The tools described in this section form the practical foundation for the implementations presented later in this thesis. Quantum teleportation, entanglement swapping, and quantum key distribution protocols can be naturally expressed as quantum circuits and analyzed through both simulation and real hardware execution.

By combining Qiskit, IBM Quantum hardware, and the Quantum Composer, it becomes possible to systematically study the impact of noise, loss, and imperfect measurements on quantum communication systems, bridging the gap between theoretical models and experimental feasibility.

Chapter 5: Satellite Link Elements

5.1 Introduction

The quantum communication algorithms and protocols discussed in the previous chapter can be realized over satellite-based communication links. In order to meaningfully analyze and assess such implementations, it is necessary to first examine the physical mechanisms and environmental factors that affect the transmission of quantum states through satellite channels.

This chapter provides a detailed overview of the key physical phenomena, constraints, and sources of impairment that arise in satellite quantum communication systems. Emphasis is placed on effects that influence the integrity, loss, and decoherence of quantum signals, as well as on practical considerations that must be taken into account when designing and operating quantum communication links involving satellites.

5.2 Uplink and downlink satellite communication

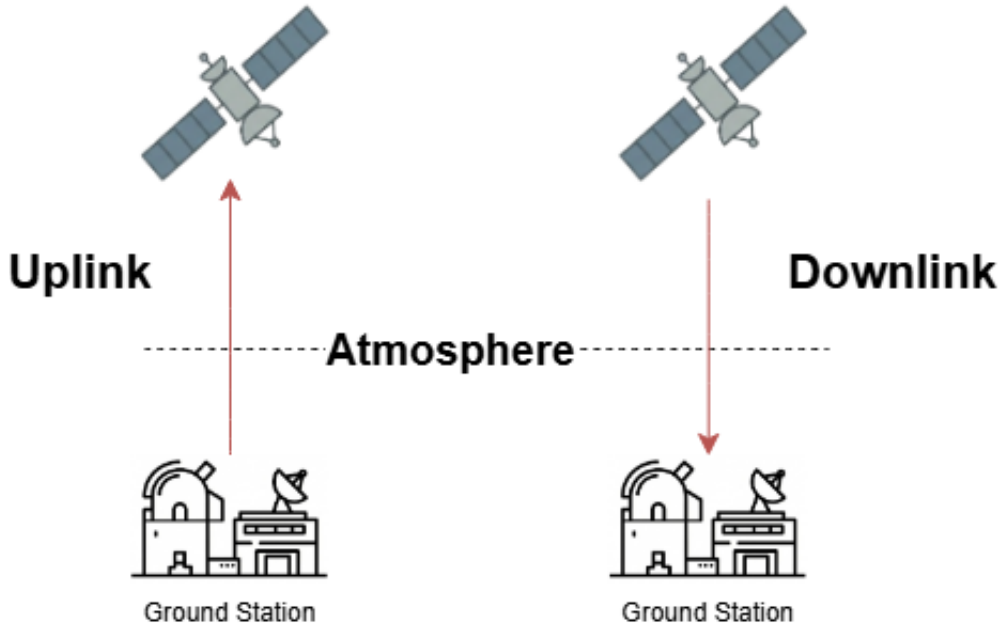

Figure 5.1: Uplink and downlink architectures

When discussing satellite-based quantum communication systems, two general architectures can be identified: **uplink** and **downlink** communication.

In uplink quantum communication schemes, the source of the qubits (photons) is located at a ground station, while the satellite acts as the receiver.

In general, uplink architectures exhibit higher losses, primarily because the dominant noisy part of the communication channel, namely the atmosphere, is located at the beginning of the optical path. This phenomenon is commonly referred to as the **shower curtain effect** [40, 41]. We will discuss in detail the physical mechanisms responsible for this effect in the following sections. An important advantage of uplink architectures is that ground-based optical stations can typically generate higher optical power and offer greater flexibility and control over qubit generation [42].

In downlink communication systems, the satellite acts as the source of the qubits and transmits quantum information to ground-based receiving stations.

The primary advantage of downlink architectures is the reduced channel loss, as the signal originates in space, where atmospheric noise and turbulence are absent. However, a key limitation of this approach is the restricted power generation and payload capabilities of satellites compared to ground-based optical stations.

5.3 Link Geometry

The geometric configuration of the satellite link is the fundamental determinant of signal attenuation, as it dictates the propagation distance through free space and the atmosphere. We consider a scenario involving a ground station A located on the Earth's surface and a satellite S orbiting at an altitude h.

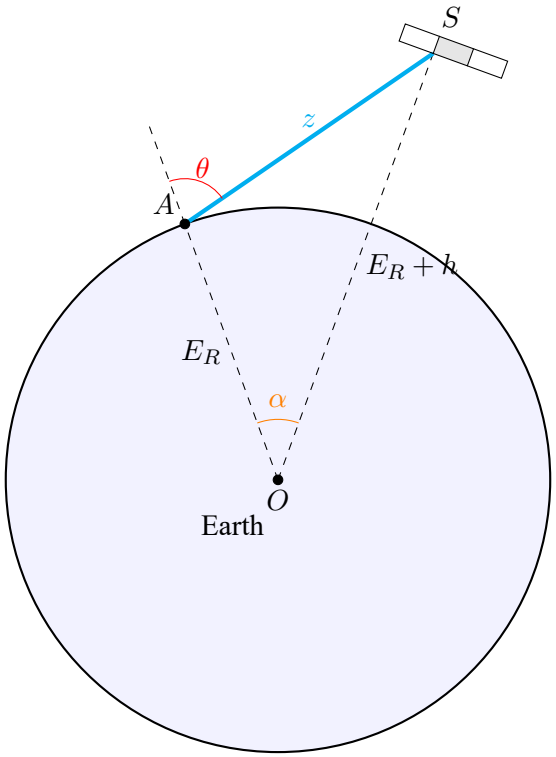

Figure 5.2: Geometry of the satellite uplink. z represents the slant range, θ is the zenith angle, and α is the central angle.

Let us define the geometric parameters of the system relative to the Earth's center O:

- E_R: The radius of the Earth (approximately 6371 km).

- h: The orbital altitude of the satellite (for LEO $\approx 160 - 2000$ km).
- θ: The zenith angle at the ground station, defined as the angle between the local vertical (zenith) and the line-of-sight to the satellite.
- z: The slant range (Euclidean distance) between the ground station and the satellite.
- α: The central angle, also called nadir angle, subtended at the Earth's center between the ground station and the satellite's nadir.

5.3.1 Slant Range Calculation

Consider the triangle $\overset{\triangle}{OAS}$ formed by the Earth's center (O), the ground station (A), and the satellite (S). The sides of this triangle are:

- $OA = E_R$
- $OS = E_R + h$
- $AS = z$

The angle $\angle OAS$ is related to the zenith angle θ. Since the zenith is perpendicular to the surface tangent, the internal angle of the triangle at vertex A is $\pi - \theta$ (assuming $\theta \leq \pi/2$).

Applying the law of cosines to $\overset{\triangle}{OAS}$:

$$OS^2 = OA^2 + AS^2 - 2(OA)(AS)\cos(\pi - \theta) \tag{5.1}$$

Substituting the physical parameters:

$$(E_R + h)^2 = E_R^2 + z^2 - 2E_R z \cos(\pi - \theta) \tag{5.2}$$

Using the identity $\cos(\pi - \theta) = -\cos\theta$, we obtain:

$$(E_R + h)^2 = E_R^2 + z^2 + 2E_R z \cos\theta \tag{5.3}$$

Rearranging to form a quadratic equation for z:

$$z^2 + (2E_R \cos\theta)z - (h^2 + 2hE_R) = 0 \tag{5.4}$$

Solving for the positive root z yields the fundamental link equation:

$$z(h, \theta) = \sqrt{h^2 + 2hE_R + E_R^2 \cos^2\theta} - E_R \cos\theta \tag{5.5}$$

This equation expresses the transmission distance strictly as a function of the satellite's altitude and its position in the sky relative to the ground station.

5.3.2 Angular Relationships

It is often useful to relate the zenith angle θ to the central angle α, which describes the satellite's position relative to the Earth's coordinate system. Using the law of cosines on the side z (side AS):

$$z^2 = E_R^2 + (E_R + h)^2 - 2E_R(E_R + h)\cos\alpha \tag{5.6}$$

Solving for $z(h, \alpha)$:

$$z(h, \alpha) = \sqrt{E_R^2 + (E_R + h)^2 - 2E_R(E_R + h)\cos\alpha} \tag{5.7}$$

By equating the two expressions for z, we can derive the mapping between the zenith angle θ and the central angle α:

$$\alpha(h, \theta) = \cos^{-1}\left[\frac{E_R + z(h, \theta)\cos\theta}{E_R + h}\right] \tag{5.8}$$

Conversely, the zenith angle can be determined from the central angle:

$$\theta(h, \alpha) = \cos^{-1}\left[\frac{(E_R + h)\cos\alpha - E_R}{z(h, \alpha)}\right] \tag{5.9}$$

5.3.3 Two Ground Station Configuration

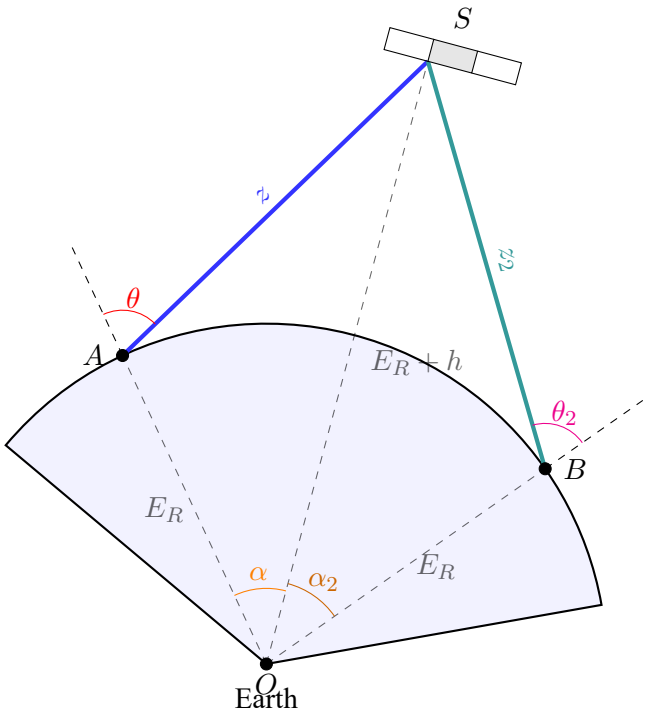

Figure 5.3: Dual-link geometry showing ground stations A and B, satellite S, and respective zenith angles θ, θ_2 and slant ranges z, z_2.

We consider two ground stations A and B separated by a great-circle distance D_G. If the satellite is positioned at an angle α relative to station A, its angle relative to station B (assuming a planar configuration

passing through the Earth's center) is:

$$\alpha_2 = \frac{D_G}{E_R} - \alpha \tag{5.10}$$

This allows us to calculate the slant range z_2 and zenith angle θ_2 for the second link independently, fully defining the geometric state of the tripartite system [43].

5.4 Beam Deformation and Turbulence Effects

As the optical beam propagates through the atmosphere, it undergoes spatial distortions that significantly reduce the photon collection probability at the receiver. These distortions are primarily classified into two phenomena [43–46]:

1. **Beam Widening:** The expansion of the beam's cross-sectional area. This is caused by two factors: the natural diffraction of light (which occurs even in a vacuum) and the scattering caused by atmospheric turbulence eddies [47, 48].

2. **Beam Wandering:** The random fluctuation of the beam's centroid (center of intensity) relative to the receiver's optical axis. This is caused by large-scale turbulent eddies acting as refractive prisms that deflect the entire beam path [43, 49].

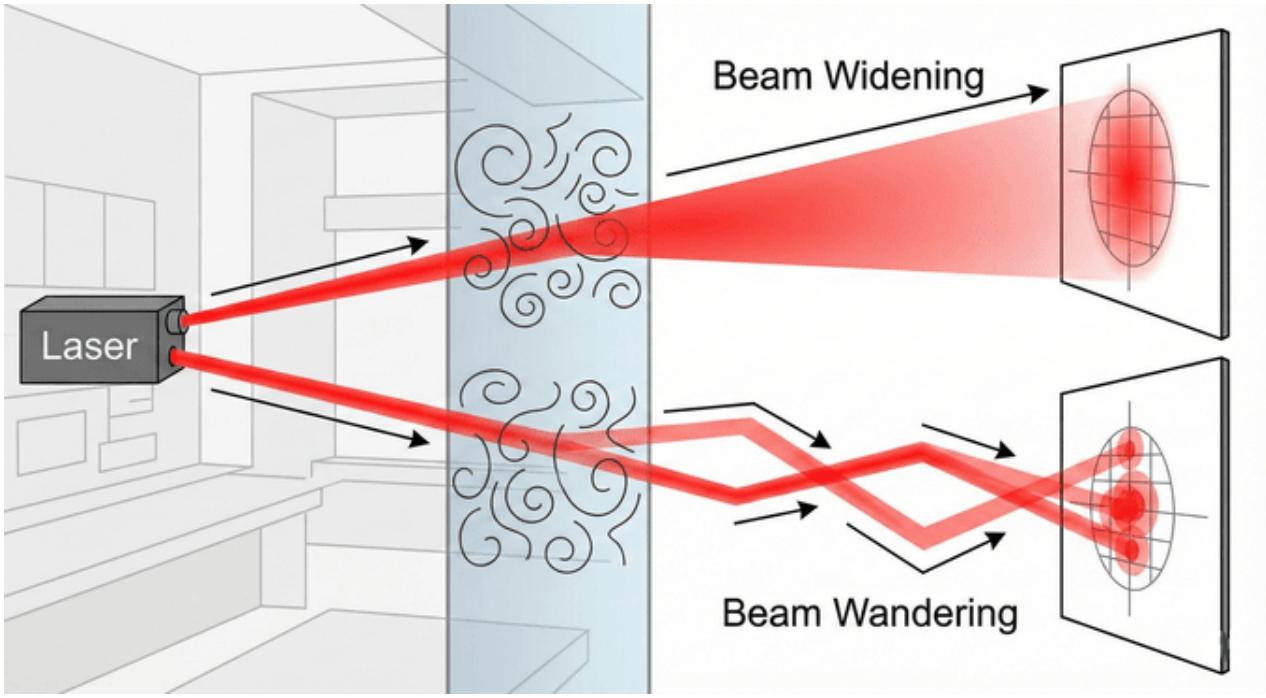

Figure 5.4: Beam widening and beam wandering

The impact of these effects is highly asymmetric between uplink and downlink configurations due to the vertical distribution of the atmosphere.

5.4.1 Uplink Scenario (Ground-to-Satellite)

In an uplink configuration, the optical beam traverses the turbulent atmospheric layer immediately upon transmission (within the first 20 km). Small angular deviations induced by refractive index fluctuations near the ground are amplified by the long propagation distance z to the satellite. Consequently, turbulence-induced Beam Wandering becomes the dominant loss mechanism [43, 46].

The effective long-term beam width w_{up} at the satellite receiver is modeled by the superposition of vacuum diffraction and turbulence-induced broadening. The squared beam radius is given by [43]:

$$w_{up}^2 = \underbrace{w_0^2 \left(1 + \left(\frac{z\lambda}{\pi w_0^2}\right)^2\right)}_{\text{Diffraction Term}} + \underbrace{2\left(\frac{\lambda z}{\pi \kappa_0}\right)^2}_{\text{Turbulence Term}} \tag{5.11}$$

where:

- w_0 is the initial beam waist radius at the ground transmitter.
- λ is the wavelength of the optical signal.
- z is the slant range (propagation distance).
- κ_0 is the turbulence-dependent coherence length.

The coherence length κ_0 encapsulates the strength of the atmospheric turbulence along the path and is highly sensitive to the zenith angle θ. It is defined as:

$$\kappa_0 = \left[1.46 \left(\frac{2\pi}{\lambda}\right)^2 \sec(\theta) \times C_w\right]^{-3/5} \tag{5.12}$$

The term $\sec(\theta)$ accounts for the increased air mass at lower elevation angles. The factor C_w represents the integrated refractive index structure constant profile (C_n^2) and typically takes values of $C_w \approx 3.28 \times 10^{-12}\, m^{1/3}$ during the day and $2.23 \times 10^{-12}\, m^{1/3}$ at night [43].

The resulting average collection efficiency η_{up}, representing the probability that a photon enters the satellite's telescope aperture R_{sat}, is given by [43]:

$$\eta_{up} = 1 - \exp\left(\frac{-2R_{sat}^2}{w_{up}^2 + \sigma_{pe}^2}\right) \tag{5.13}$$

where σ_{pe} accounts for the pointing and tracking errors of the transmitter.

5.4.2 Downlink Scenario (Satellite-to-Ground)

In a downlink configuration, the beam propagates through the vacuum of space and encounters the atmosphere only at the very end of its path. Since the distance from the turbulent layer to the receiver (ground station) is negligible compared to the total slant range z, the angular deviations induced by turbulence

do not have sufficient distance to translate into significant spatial displacements (Beam Wandering is minimized).

Therefore, for the downlink channel, the turbulence term in Eq. 5.11 becomes negligible. The beam width w_{down} at the ground receiver is dominated by the geometric diffraction limit [43]:

$$w_{down}^2 \approx w_0^2 \left(1 + \left(\frac{z\lambda}{\pi w_0^2}\right)^2\right) \tag{5.14}$$

Although diffraction still causes the beam to spread significantly due to the large distance z, the absence of severe beam wandering allows for a more stable link. Furthermore, ground stations can employ significantly larger telescope apertures ($R_{ground} \gg R_{sat}$) to compensate for the diffractive spreading, resulting in a collection efficiency η_{down}:

$$\eta_{down} = 1 - \exp\left(\frac{-2R_{ground}^2}{w_{down}^2 + \sigma_{pe}^2}\right) \tag{5.15}$$

Comparing Eq. 5.11 and Eq. 5.14, it is evident that the downlink configuration offers superior channel stability by effectively eliminating the turbulence-induced broadening term $2(\frac{\lambda z}{\pi \kappa_0})^2$.

5.5 Stray Photons and Background Noise

In quantum communications implementations involving Low Earth Orbit (LEO) satellites, the signal-to-noise ratio (SNR) is a critical parameter. Since the signal consists of single photons or weak coherent pulses, background noise can severely degrade the Quantum Bit Error Rate (QBER). This section analyzes the background noise contributions for both uplink and downlink configurations, distinguishing between day-time and night-time operations. The models presented herein are based on the analysis by Bonato *et al.* [45].

5.5.1 Uplink Configuration (Ground-to-Satellite)

In the uplink scenario, the receiving telescope is located on the satellite, pointing towards the Earth. The background noise is dominated by light reflected from the Earth's surface or emitted by the Earth itself.

Day-time Operation During day-time, the primary noise source is solar radiation reflected by the Earth's albedo into the satellite telescope's field of view (FOV). Assuming the Earth behaves as a Lambertian diffuser, the spectral radiance L_E (photons $\cdot$ s^{-1} $\cdot$ nm^{-1} $\cdot$ m^{-2} $\cdot$ sr^{-1}) reflected by the Earth is given by [45]:

$$L_E = \frac{1}{\pi} a_E H_{sun} \tag{5.16}$$

where a_E is the Earth's albedo and H_{sun} is the solar spectral irradiance (photons $\cdot$ s^{-1} $\cdot$ nm^{-1} $\cdot$ m^{-2}).

For a satellite at an altitude z, equipped with a telescope of radius R_{sat} and an angular instantaneous field-of-view ($IFOV$), the observed area Σ on Earth and the solid angle Ω_{sat} subtended by the telescope are related by geometric optics. The total number of background photons N_{day}^{up} collected per second is obtained by integrating the radiance over the observed area, the solid angle of the receiver, and the spectral bandwidth $\Delta\lambda$:

$$N_{day}^{up} = L_E \times \Sigma \times \Omega_{sat} \times \Delta\lambda \tag{5.17}$$

Substituting the geometric approximations $\Sigma \approx (IFOV \cdot z)^2$ and $\Omega_{sat} \approx \pi R_{sat}^2/z^2$, the dependence on the link distance z cancels out, yielding [45]:

$$N_{day}^{up} = \frac{1}{\pi} a_E H_{sun} (IFOV \cdot z)^2 \frac{\pi R_{sat}^2}{z^2} \Delta\lambda = a_E H_{sun} R_{sat}^2 (IFOV)^2 \Delta\lambda \tag{5.18}$$

This equation demonstrates that background noise in the uplink is governed by the telescope's intake area and the square of the field of view, and is independent of the satellite's altitude.

Night-time Operation During night-time, the background noise is significantly reduced. The three main sources are reflected moonlight, the Earth's thermal black-body emission, and anthropogenic light pollution.

The contribution from moonlight is modeled as a two-stage reflection process. The spectral radiance reflected by the Moon, L_M, leads to an effective radiance from the Earth's surface $L_E^{(M)}$ [45]:

$$L_E^{(M)} = \frac{1}{\pi} a_E \left(\frac{1}{\pi} a_M H_{sun} \frac{\pi R_M^2}{d_{EM}^2} \right) \tag{5.19}$$

Consequently, the number of photons collected by the satellite telescope at night, N_{night}^{up}, can be expressed as a fraction of the day-time noise:

$$N_{night}^{up} = \alpha N_{day}^{up} \tag{5.20}$$

where the scaling factor α is defined as $\alpha = a_M (R_M/d_{EM})^2$. Given typical values [45] ($a_M \approx 0.12$), $\alpha \approx 10^{-6}$, indicating a six-order-of-magnitude noise reduction.

Regarding thermal noise, the Earth emits black-body radiation ($T \approx 293$ K). According to Planck's law, the spectral radiance $L_{BB}(\lambda)$ is:

$$L_{BB}(\lambda) = \frac{2c}{\lambda^4} \frac{1}{e^{hc/(\lambda k_B T)} - 1} \tag{5.21}$$

At typical QKD wavelengths ($\lambda \approx 800$ nm), the thermal photon count is negligible compared to the moonlight contribution.

5.5.2 Downlink Configuration (Satellite-to-Ground)

In the downlink configuration, the ground station telescope points towards the satellite against the sky background. The background noise rate N_b^{down} received by the telescope is modeled as [50]:

$$N_b^{down} = H_{sky}\Omega_{fov}\pi R_{rec}^2\Delta\lambda \tag{5.22}$$

where:

- H_{sky} is the sky spectral radiance (photons $\cdot$ s^{-1} $\cdot$ m^{-2} $\cdot$ sr^{-1} $\cdot$ nm^{-1}),
- Ω_{fov} is the receiver's solid angle field of view (sr),
- R_{rec} is the radius of the receiving ground telescope,
- $\Delta\lambda$ is the spectral filter bandwidth.

Unlike the uplink, the value of H_{sky} varies drastically. It ranges from $\sim 1.5 \times 10^{-6}$ W$\cdot$m$^{-2}\cdot$sr$^{-1}\cdot$nm^{-1} at night to $\sim 1.5 \times 10^{-3}$ during the day [50]. This asymmetry necessitates extreme spatial and spectral filtering for daylight downlink operations.

5.6 Atmospheric Attenuation

As optical signals propagate through the Earth's atmosphere, they experience extinction due to absorption and scattering by air molecules and aerosols. Unlike turbulence-induced errors, which are asymmetric, atmospheric attenuation acts as a reciprocal loss mechanism, affecting both uplink and downlink channels equally based on the total optical depth.

The transmissivity of the atmospheric channel, denoted as η_{atm}, is modeled using the Beer-Lambert law [43]. It depends on the wavelength λ and the path integral of the extinction coefficient along the propagation trajectory. For a satellite link with zenith angle θ, the transmissivity is given by [43]:

$$\eta_{atm}(h,\theta) = \exp\left[-\alpha_0(\lambda)\int_0^{z(h,\theta)} \exp\left(-\frac{h(y,\theta)}{\tilde{h}}\right) dy\right] \tag{5.23}$$

where:

- $\alpha_0(\lambda)$: The extinction coefficient at sea level (typically $\approx 10^{-4}\, m^{-1}$ for clear days at optical wavelengths).
- $z(h,\theta)$: The total slant range distance to the satellite.

- $\tilde{h}$: The atmospheric scale height (typically ≈ 6600 m), representing the altitude at which atmospheric density drops by a factor of $1/e$.
- $h(y, \theta)$: The altitude of the beam at a distance y along the path.

The integral reflects the fact that the beam passes through atmospheric layers of varying density. At the zenith ($\theta = 0°$), the path through the dense lower atmosphere is minimized, resulting in maximum transmissivity. As θ increases toward the horizon, the effective air mass increases roughly as $\sec(\theta)$, leading to a sharp exponential decay in signal strength.

For practical simulations at $\lambda \approx 800$ nm under clear weather conditions, the atmospheric transmittance at zenith is typically $\eta_{atm}^{zenith} \approx 0.8$ (or -1 dB), but can drop below 0.1 (-10 dB) at low elevation angles ($\theta > 70°$).

5.7 Mode Mismatch and Temporal Synchronization

In this section, we isolate the effects of spatiotemporal mode mismatch [51, 52], assuming that all other noise sources (such as beam widening, wandering, and stray photons) are negligible.

For the successful execution of optical Bell State Measurements (BSM), it is imperative that the two photons arriving from the ground stations are indistinguishable. They must align perfectly in the spatiotemporal domain to exhibit quantum interference. A temporal mismatch Δt between the arrival times of the two wavepackets increases their distinguishability, thereby reducing the fidelity of the swapped entanglement.

To mitigate this, a time-gating window is employed. This window activates the detectors only for a limited duration, ensuring that only the overlapping segments of the wavepackets are detected. This involves a trade-off: a narrower window reduces distinguishability (improving fidelity) but also discards a portion of the signal (reducing success probability).

5.7.1 Wavepacket Formalism

Physically, a photon located at position x_0 is described by a Gaussian wavepacket $\psi(x)$ with a spatial amplitude distribution is given by [53]:

$$\psi(x) = \left(\frac{1}{2\pi\sigma^2}\right)^{\frac{1}{4}} e^{-\frac{1}{4}\left(\frac{x-x_0}{\sigma}\right)^2} e^{ik(x-x_0)} \tag{5.24}$$

where $\sigma = c\sigma_t$ relates the spatial width to the temporal width σ_t, $k = 2\pi/\lambda$ is the wavenumber, and c is the speed of light. When two photons arrive with a time difference $\Delta t = t_2 - t_1$, this corresponds to a path difference $\Delta x = c\Delta t$. Thus, the second wavepacket is shifted relative to the first: $\psi_2(x) = \psi_1(x + \Delta x)$.

5.7.2 State Evolution and Time-Gating

The photons pass through the BSM optical setup (Polarizing Beam Splitter and Half-Wave Plates) and are detected within a time window $[t_{min}, t_{max}]$. This process is mathematically represented by the time-

gating projection operator $\hat{T}(\tau)$ [46]:

$$\hat{T}(\tau) = \int_{ct_{min}}^{ct_{max}} \hat{a}^\dagger(x)|0\rangle\langle 0|\hat{a}(x)\, dx \tag{5.25}$$

After the measurement and tracing out the optical modes (since the remaining temporal information is inaccessible), the state is described by the reduced density matrix $\hat{\rho}_{mm}$ [46]:

$$\hat{\rho}_{mm} = \frac{1}{4}\Big[\zeta|HH\rangle\langle HH| + (-1)^p\gamma|HH\rangle\langle VV| + (-1)^p\gamma|VV\rangle\langle HH| + \zeta|VV\rangle\langle VV|\Big] \tag{5.26}$$

where p represents the parity of the measurement outcome. The parameters ζ and γ quantify the signal collection and the interference quality, respectively:

$$\zeta = \left(\int_{ct_{min}}^{ct_{max}} |\psi_1(x)|^2 dx\right)\left(\int_{ct_{min}}^{ct_{max}} |\psi_2(x)|^2 dx\right), \quad \gamma = \left|\int_{ct_{min}}^{ct_{max}} \psi_1(x)\psi_2^*(x)\, dx\right|^2 \tag{5.27}$$

5.7.3 Gating Probability and Final Fidelity

The term ζ can be expressed as the product of the probabilities that each individual photon passes through the gating window. The gating probability P_{gw_i} for mode i is [46]:

$$P_{gw_i} = \int_{ct_{min}}^{ct_{max}} |\psi_i(x)|^2 dx \tag{5.28}$$

Thus, $\zeta = P_{gw_1}P_{gw_2}$.

The fidelity is defined as the overlap between the ideal target quantum state and the received quantum state, and serves as a key indicator of entanglement quality in noisy quantum communication channels.

The Fidelity F_{ic} (under ideal channel assumptions) is calculated by comparing the resulting density matrix $\hat{\rho}_{mm}$ with the ideal Bell state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + (-1)^p|VV\rangle)$. The final expression for the fidelity depends on the ratio of the interference term γ to the collection probabilities [46]:

$$F_{ic} = \frac{\langle\Phi|\hat{\rho}_{mm}|\Phi\rangle}{\text{tr}(\hat{\rho}_{mm})} = \frac{1}{2} + \frac{\gamma}{2P_{gw_1}P_{gw_2}} \tag{5.29}$$

This equation encapsulates the impact of mode mismatch: if the overlap is perfect ($\gamma = \zeta$), the fidelity reaches 1. As the mismatch Δx increases or the gate cuts off the interference tails, the ratio $\gamma/(P_{gw_1}P_{gw_2})$ decreases, degrading the fidelity towards the classical limit of 0.5.

Chapter 6: Entanglement Distribution via Satellite Link

6.1 Introduction

In the following chapter, we propose various architectures for distributing entanglement between two ground stations, Alice and Bob, via satellite links. For each architecture, a detailed feasibility analysis is presented, utilizing the link elements discussed in the previous chapter to realistically simulate the performance and requirements.

Initially, we analyze a well-established uplink configuration in which each ground station generates an entangled qubit pair and transmits one qubit to a satellite, where entanglement swapping is performed. Subsequently, we propose underexplored satellite-assisted configurations and evaluate their feasibility under realistic noise and synchronization constraints. This is the novel contribution of this thesis.

6.2 Single-Satellite Dual Uplink Network

6.2.1 Architectural Design

The network consists of three primary nodes:

- Ground station Alice (A)
- Ground station Bob (B)
- A single LEO satellite in common view of both ground stations.

The objective is to establish an entangled qubit pair between Alice and Bob by employing the entanglement swapping protocol.

Step 1: Entangled qubit pair generation

Alice and Bob each generate an entangled qubit pair in the Bell state:

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{6.1}$$

Alice holds the entangled qubit pair (q_0,q_1), while Bob holds the entangled qubit pair (q_2,q_3). The ultimate goal is to entangle the distant qubits q_0 and q_3, without any direct interaction between them. Without loss of generality we can assume that Alice and Bob have agreed to have the paired (q_0,q_3) entangled in the Bell state $|\Phi^{+}\rangle_{03}$.

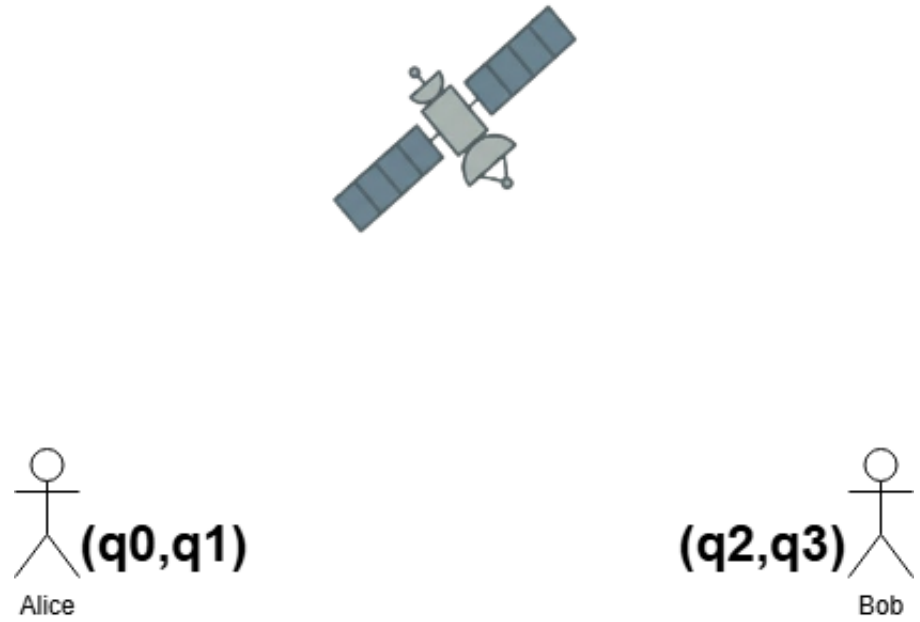

Figure 6.1: Both Alice and Bob generate an entangled qubit pair

The initial state of the joint quantum system is:

$$\begin{aligned} |\psi_0\rangle &= \left|\Phi^+\right\rangle_{01} \otimes \left|\Phi^+\right\rangle_{23} \\ &= \frac{1}{2}\left[|0000\rangle_{0123} + |0011\rangle_{0123} + |1100\rangle_{0123} + |1111\rangle_{0123}\right] \\ &= \frac{1}{2}[|00\rangle_{03} \otimes |00\rangle_{12} + |01\rangle_{03} \otimes |01\rangle_{12} + |10\rangle_{03} \otimes |10\rangle_{12} + |11\rangle_{03} \otimes |11\rangle_{12}] \end{aligned} \tag{6.2}$$

By expanding the computational basis states into the Bell basis using the following relations:

$$\begin{aligned} |00\rangle = \frac{1}{\sqrt{2}}[\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle], \quad |01\rangle = \frac{1}{\sqrt{2}}[\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle] \\ |10\rangle = \frac{1}{\sqrt{2}}[\left|\Psi^+\right\rangle - \left|\Psi^-\right\rangle], \quad |11\rangle = \frac{1}{\sqrt{2}}[\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle], \end{aligned} \tag{6.3}$$

the total state $|\psi_0\rangle$ can be decomposed to highlight the correlations between the $(0,3)$ and $(1,2)$ qubit pairs as:

$$\begin{aligned} |\psi_0\rangle = \frac{1}{4}[&\left|\Phi^+\right\rangle_{03} \otimes \left|\Phi^+\right\rangle_{12} + \left|\Phi^+\right\rangle_{03} \otimes \left|\Phi^-\right\rangle_{12} + \left|\Phi^-\right\rangle_{03} \otimes \left|\Phi^+\right\rangle_{12} + \left|\Phi^-\right\rangle_{03} \otimes \left|\Phi^-\right\rangle_{12} \\ &+ \left|\Psi^+\right\rangle_{03} \otimes \left|\Psi^+\right\rangle_{12} + \left|\Psi^+\right\rangle_{03} \otimes \left|\Psi^-\right\rangle_{12} + \left|\Psi^-\right\rangle_{03} \otimes \left|\Psi^+\right\rangle_{12} + \left|\Psi^-\right\rangle_{03} \otimes \left|\Psi^-\right\rangle_{12} \\ &+ \left|\Psi^+\right\rangle_{03} \otimes \left|\Psi^+\right\rangle_{12} - \left|\Psi^+\right\rangle_{03} \otimes \left|\Psi^-\right\rangle_{12} - \left|\Psi^-\right\rangle_{03} \otimes \left|\Psi^+\right\rangle_{12} + \left|\Psi^-\right\rangle_{03} \otimes \left|\Psi^-\right\rangle_{12} \\ &+ \left|\Phi^+\right\rangle_{03} \otimes \left|\Phi^+\right\rangle_{12} - \left|\Phi^+\right\rangle_{03} \otimes \left|\Phi^-\right\rangle_{12} - \left|\Phi^-\right\rangle_{03} \otimes \left|\Phi^+\right\rangle_{12} + \left|\Phi^-\right\rangle_{03} \otimes \left|\Phi^-\right\rangle_{12}] \\ = \frac{1}{2}[&\left|\Phi^+\right\rangle_{03} \otimes \left|\Phi^+\right\rangle_{12} + \left|\Phi^-\right\rangle_{03} \otimes \left|\Phi^-\right\rangle_{12} + \left|\Psi^+\right\rangle_{03} \otimes \left|\Psi^+\right\rangle_{12} + \left|\Psi^-\right\rangle_{03} \otimes \left|\Psi^-\right\rangle_{12}] \end{aligned} \tag{6.4}$$

Step 2: Qubit transfer to satellite

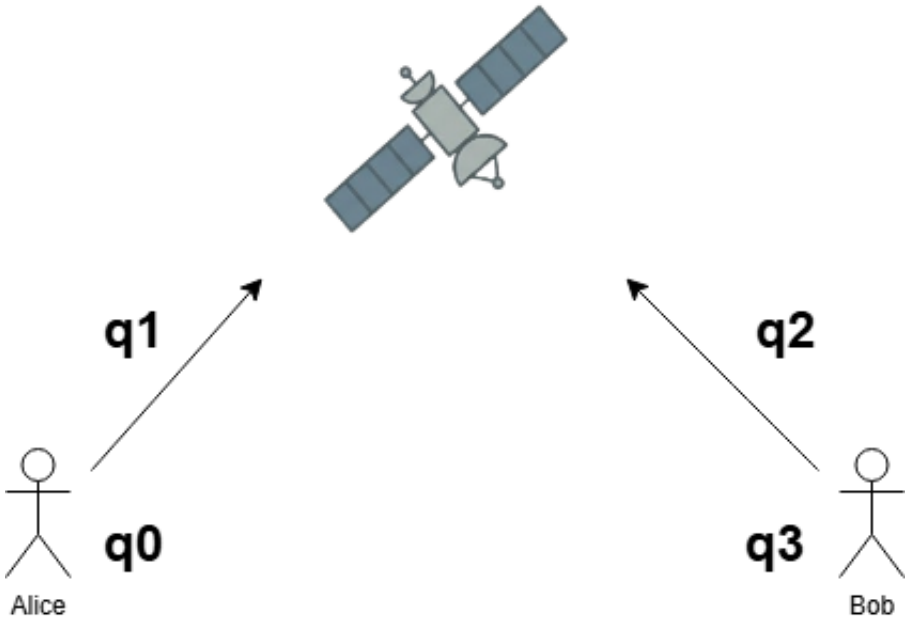

Figure 6.2: Alice and Bob each send a qubit to the satellite

Qubits q_1 and q_2 are transmitted from their respective ground stations to the satellite receiver. To entangle the target qubits q_0 and q_3, the satellite must perform a Bell State Measurement (BSM) on qubits q_1 and q_2, which have just arrived on its detectors.

Step 3: Bell-state measurement

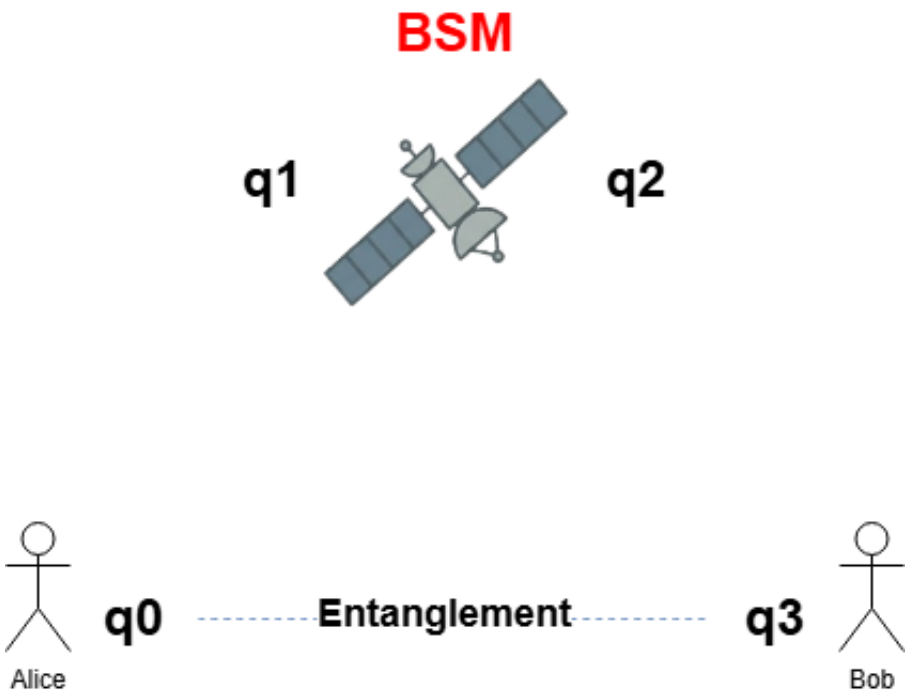

Figure 6.3: The satellite performs a BSM

The satellite performs a BSM on qubits q_1 and q_2. Since a BSM projects the joint state into one of the four Bell states, it follows from Eq. (6.4) that the measurement yields one of the four equally probable outcomes ($|\Phi^+\rangle_{03}, |\Phi^-\rangle_{03}, |\Psi^+\rangle_{03}, |\Psi^-\rangle_{03}$).

Upon measurement, the state of the system collapses. Crucially, the remaining qubits q_0 and q_3 at the ground stations become entangled in a state that corresponds to the BSM outcome. For instance, if the satellite detects the state $|\Phi^-\rangle_{12}$, the ground-based qubits collapse into the $|\Phi^-\rangle_{03}$ state.

Step 4: Local Correction

Alice and Bob now possess an entangled pair, but the specific state depends on the random BSM outcome. To ensure that the deterministic final state is $|\Phi^+\rangle_{03}$ as they agreed, a correction phase is required. The satellite communicates the BSM result to Alice via a classical channel, who then applies the appropriate Pauli gates.

Consider an example where the BSM yields the outcome $|\Psi^-\rangle_{12}$. The classical bit sequence for this state is derived by applying a CNOT gate (with q_1 as control and q_2 as target):

$$CNOT\left|\Psi^-\right\rangle_{12} = \frac{1}{\sqrt{2}} CNOT(|01\rangle_{12} - |10\rangle_{12}) = \frac{1}{\sqrt{2}}(|01\rangle_{12} - |11\rangle_{12}) \tag{6.5}$$

followed by a Hadamard gate on q_1:

$$\begin{aligned}(H \otimes I)(CNOT\left|\Psi^-\right\rangle_{12}) &= \frac{1}{\sqrt{2}}(H \otimes I)(|01\rangle_{12} - |11\rangle_{12}) \\ &= \frac{1}{2}\left[(|0\rangle_1 + |1\rangle_1)\,|1\rangle_2 - (|0\rangle_1 - |1\rangle_1)\,|1\rangle_2\right] \\ &= \frac{1}{2}(|01\rangle_{12} + |11\rangle_{12} - |01\rangle_{12} + |11\rangle_{12}) = |11\rangle_{12}\end{aligned} \tag{6.6}$$

The resulting classical outcome is 11.

Table 6.1: Mapping of Bell states to classical measurement outcomes.

Bell State	**Mathematical Expression**	**After CNOT**	**After $H \otimes I$**	**Outcome ($q_1 q_2$)**
$\|\Phi^+\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\|00\rangle$	**00**
$\|\Phi^-\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\|10\rangle$	**10**
$\|\Psi^+\rangle$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle + \|11\rangle)$	$\|01\rangle$	**01**
$\|\Psi^-\rangle$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|11\rangle)$	$\|11\rangle$	**11**

Upon receiving this signal, Alice knows the shared state is $|\Psi^-\rangle_{03}$. To transform this into the desired

$|\Phi^+\rangle$ state, she applies a Pauli-X gate followed by a Pauli-Z gate to her qubit q_0:

$$\begin{aligned} Z_0 X_0 \left|\Psi^-\right\rangle_{03} &= Z_0 X_0 \left[\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\right] \\ &= Z_0 \left[\frac{1}{\sqrt{2}}(|11\rangle - |00\rangle)\right] \\ &= \frac{1}{\sqrt{2}}(-|11\rangle - |00\rangle) \equiv \left|\Phi^+\right\rangle_{03} \text{ (up to a global phase)} \end{aligned} \tag{6.7}$$

The correction mapping is summarized in Table 6.2.

Table 6.2: Measurement outcome and corresponding local correction (desired state $|\Phi^+\rangle$)

Measurement Outcome	Correction
$\|00\rangle$	Identity gate I
$\|01\rangle$	Pauli-X gate
$\|10\rangle$	Pauli-Z gate
$\|11\rangle$	Pauli-X gate followed by Pauli-Z gate

6.2.2 Feasibility Analysis under Realistic Conditions

Having defined the protocol in an ideal setting, we now evaluate its performance in a realistic scenario. The transition from theory to practice requires accounting for the physical limitations of the channel and the equipment. We adopt the comprehensive model presented by Srikara *et al.* [46], which incorporates atmospheric effects, stray photons, and mode mismatch to derive the Overall Success Probability (η_{tot}) and the Practical Fidelity (F).

6.2.2.1 Overview of Practical Impairments

Before deriving the analytical expressions for the system's performance metrics, we briefly summarize the primary physical mechanisms that degrade the link efficiency and fidelity:

- **Geometric and Atmospheric Losses:** The uplink transmission is severely affected by the turbulent atmosphere. Refractive index fluctuations cause *beam wandering* (random displacement of the beam centroid) and *beam widening* (spreading of the beam profile), significantly reducing the probability of photon collection at the satellite's aperture. Additionally, atmospheric extinction leads to direct photon loss due to absorption and scattering [46].
- **Background Noise and Stray Photons:** The satellite receiver is exposed to external sources of radiation, including reflected sunlight (albedo), moonlight, and Earth's thermal emission. These stray photons, along with the intrinsic dark counts of the detectors, introduce false detection events (noise). The rate of these events varies drastically between day and night operation, imposing strict limits on the achievable Signal-to-Noise Ratio (SNR) [46].

- **Spatiotemporal Mode Mismatch:** For the Bell State Measurement (BSM) to succeed, the photons arriving from ground stations A and B must be indistinguishable. However, path length variations and synchronization errors lead to a temporal mismatch Δt between the arriving wavepackets. This distinguishability reduces the total fidelity [46].

6.2.2.2 Model Assumptions

To simplify the analytical model while retaining the core physical dynamics, we make the following assumptions based on the literature [46]:

- **Symmetric Geometry:** We consider the snapshot where the satellite is equidistant from the two ground stations ($z_A = z_B$). This symmetry assumption simplifies the calculation of channel efficiencies without loss of generality for the feasibility assessment.
- **Polarization & Doppler:** We ignore polarization errors as they are negligible ($< 0.06\%$) [46, 54], and we assume that Doppler shifts are compensated by precise wavelength calibration [46, 55, 56].

Finally, it must be emphasized that our analysis is exclusively focused on nighttime operation. Quantitative assessments of daytime quantum uplinks consistently indicate that such links are currently prohibitive due to the overwhelming solar background noise [46, 57].

6.2.2.3 Overall Success Probability (η_{tot})

To evaluate the success probability of the entanglement swapping protocol, we consider a standard linear-optical Bell State Measurement (BSM) implementation. Such a setup typically employs a beam splitter to mix the two input modes (one from Alice and one from Bob), followed by polarization-resolving detection stages (see figure 6.4 [46]) . This results in four distinct detection channels, which we denote as D_1, D_2 (corresponding to the first input mode's outputs) and D_3, D_4 (corresponding to the second input mode's outputs).

The fundamental challenge in this configuration is that the single-photon detectors cannot distinguish between a "legitimate" photon arriving from a ground station and a "stray" photon originating from background noise. Consequently, a "successful" detection event is defined solely by the pattern of clicks registered by the detectors, regardless of their origin.

We define the detection state as a tuple $d = (d_1, d_2, d_3, d_4)$, where $d_i \in \{0, 1\}$ denotes a no-click (0) or click (1) event for the i-th detector. For the BSM to be considered successful, the detection logic must register a valid coincidence signature M. A typical valid signature for a Bell state projection (e.g. onto $|\Psi^-\rangle$) corresponds to a coincidence click between the two output arms, such as $M = (1, 0, 1, 0)$ (i.e., detector D_1 and detector D_3 click simultaneously).

The probability of observing such a signature arises from the superposition of two independent processes: the arrival of signal photons (denoted by G) and the arrival of noise photons (denoted by D). A detector

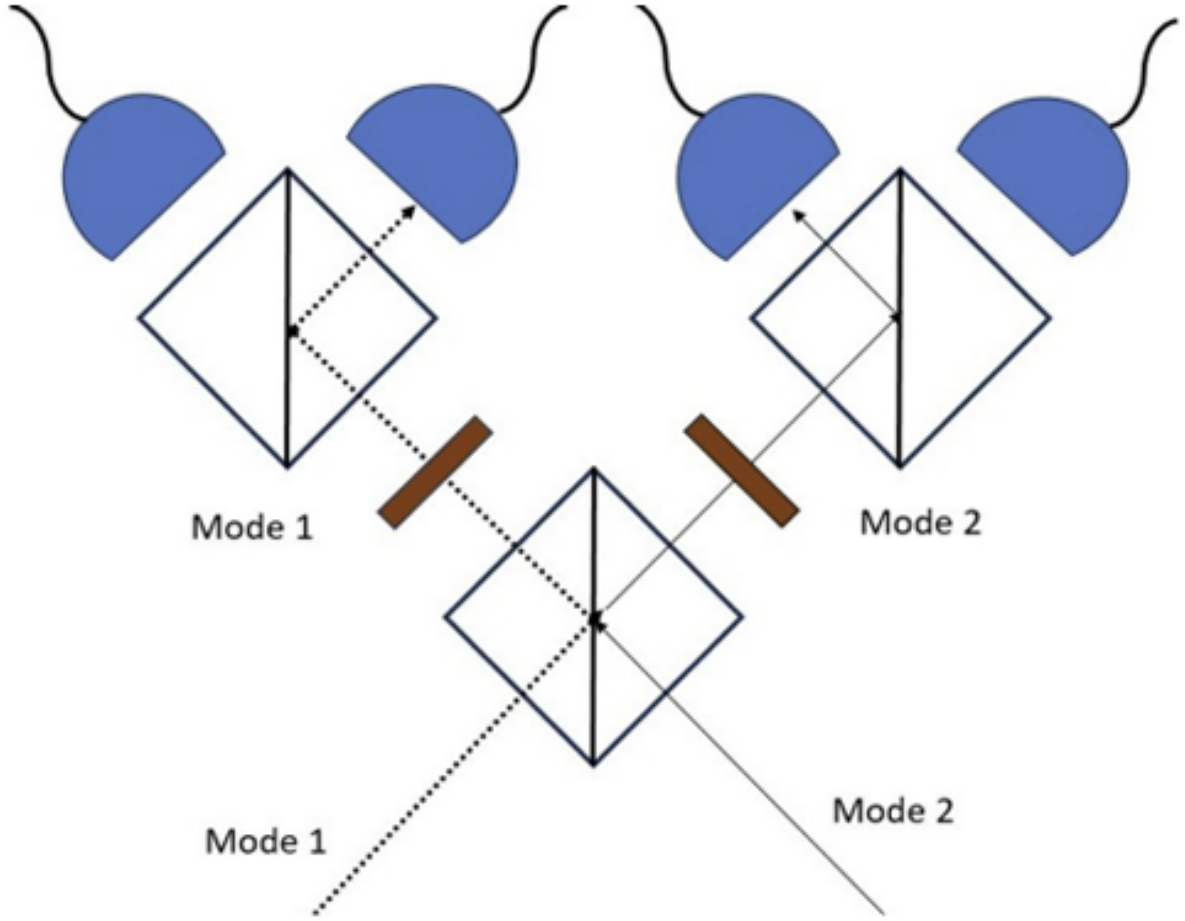

Figure 6.4: Bell state measurement implementation inside the satellite.

i fires if it receives a photon from the ground *OR* a noise photon (i.e., $d_i = g_i \vee n_i$). Therefore, a specific success pattern can be generated by multiple mutually exclusive combinations of signal and noise.

Taking the signature $M = (1,0,1,0)$ as an example, the probability $P_M(1,0,1,0)$ is calculated by summing the probabilities of all disjoint scenarios where the combination of signal and noise results in clicks at detectors 1 and 3, and silence at detectors 2 and 4 [46]:

$$\begin{aligned} P_M(1,0,1,0) = & \underbrace{P_G(1,0,1,0)}_{\text{Signal only}} \times \underbrace{[P_D(0,0,0,0) + P_D(0,0,1,0) + P_D(1,0,0,0) + P_D(1,0,1,0)]}_{\text{Noise does not trigger } d_2, d_4} \\ & + \underbrace{P_G(0,0,1,0)}_{\text{Signal at } d_3} \times \underbrace{[P_D(1,0,0,0) + P_D(1,0,1,0)]}_{\text{Noise triggers } d_1 \text{ (and optionally } d_3)} \\ & + \underbrace{P_G(1,0,0,0)}_{\text{Signal at } d_1} \times \underbrace{[P_D(0,0,1,0) + P_D(1,0,1,0)]}_{\text{Noise triggers } d_3 \text{ (and optionally } d_1)} \\ & + \underbrace{P_G(0,0,0,0)}_{\text{No Signal}} \times \underbrace{P_D(1,0,1,0)}_{\text{Pure Noise}} \end{aligned} \tag{6.8}$$

This expansion reveals the vulnerability of the protocol to noise.

- The **first term** represents the ideal case where the signal provides the correct clicks, and the noise is either absent or hits the already-active detectors.
- The **middle terms** represent "hybrid" coincidences, where one valid photon arrives from a ground station, but the second required click is triggered by noise.
- The **last term** represents a "noisy coincidence" where no signal photons arrive, but random noise triggers the exact pattern of a Bell state.

Although all these events contribute to the overall detection rate (Efficiency), only the first term represents useful entanglement. The others introduce errors that degrade the Fidelity.

Assuming a symmetric optical implementation, there are four such valid signatures (e.g. 1010, 1001, 0110, 0101). Thus, the **Total Uplink Efficiency** is given by summing the probabilities of all valid signatures [46]:

$$\eta_{tot} = 4 \times P_M(1, 0, 1, 0) \tag{6.9}$$

6.2.2.4 Practical Fidelity (F)

While the Overall Success Probability (η_{tot}) quantifies how often the satellite registers a valid detection signature, the *Fidelity* (F) quantifies the quality of the distributed entanglement in those successful events. In an ideal noise-free environment, the fidelity is limited only by the spatiotemporal indistinguishability of the photons. However, in a realistic uplink channel, background noise introduces "false positive" signatures that severely degrade the purity of the final state.

We define the Practical Fidelity F as a weighted average of the fidelity of "legitimate" events and "illegitimate" events. Let P_S be the conditional probability that a recorded valid signature (e.g. $M = (1, 0, 1, 0)$) is caused by actual signal photons from the ground stations, rather than stray light or dark counts. This probability essentially represents the Signal-to-Noise Ratio (SNR) of the detection logic.

The final state distributed between Alice and Bob, ρ_{final}, is a mixture of the desired entangled state (created when signal photons interfere) and a maximally mixed state (created when noise triggers the detectors). The fidelity is given by [46]:

$$F = P_S F_{ic} + (1 - P_S) F_{noise} \tag{6.10}$$

Physical Interpretation of Terms:

- F_{ic} **(Ideal Coincidence Fidelity):** This term represents the fidelity achieved when the detection is genuine. It is governed by the *Mode Mismatch* between the two signal wavepackets. As previously discussed, if the photons arrive with a time delay Δt, the interference visibility drops, and F_{ic} is calculated as:

$$F_{ic} = \frac{1}{2} + \frac{\gamma}{2P_{gw_1}P_{gw_2}} \tag{6.11}$$

where γ is the overlap integral and P_{gw} is the gating probability. If synchronization is perfect, $F_{ic} \to 1$.

- F_{noise} **(Noise Floor):** This term represents the fidelity when the detection signature is triggered by uncorrelated noise (e.g. stray photons or dark counts). In this case, the resulting state is the maximally mixed state $I/4$. The fidelity of any Bell state with respect to the maximally mixed state is the classical limit:

$$F_{noise} = \frac{1}{4} = 0.25 \tag{6.12}$$

- P_S **(Signal Probability):** This is the crucial weighting factor. It is the ratio of the "Signal-only" probability to the total probability of observing the signature (derived in Eq. 6.8):

$$P_S = \frac{P_G(1,0,1,0) \times P_D(0,0,0,0)}{P_M(1,0,1,0)} \tag{6.13}$$

Substituting these into Eq. 6.10, the final expression for Practical Fidelity becomes [46]:

$$F = P_S \left(\frac{1}{2} + \frac{\gamma}{2P_{gw_1}P_{gw_2}} \right) + \frac{1 - P_S}{4} \tag{6.14}$$

This equation demonstrates the dual dependency of the system:

1. If the **synchronization is poor** ($\gamma \to 0$), the first term drops to $0.5P_S$, limiting the maximum achievable fidelity.
2. If the **noise is high** (e.g. during daytime or high turbulence), $P_S \to 0$. In this regime, the fidelity collapses towards the classical limit of 0.25, rendering the distributed state useless for quantum communication.

6.2.2.5 Fixed Simulation Parameters

Table 6.3: System parameters and environmental conditions used for numerical simulations.

Parameter	**Symbol**	**Value**	**Reference**
Satellite aperture diameter	D	150 cm	[58, 59]
Operating wavelength	λ	800 nm	[58]
Detector efficiency	η_{det}	≈ 0.6	[58]
Total measurement efficiency	η_{meas}	0.25	[58]
PBS transmissivity	η_{pbs}	~ 0.91	[58]
BSM efficiency factor (45° waveplate)	-	0.5	[58]
Earth surface temperature	T	300 K (27°C)	-
Clock synchronization precision	Δt_{sync}	3 ns	[58, 60]

For the numerical simulations, we fix several key system parameters based on realistic hardware capabilities and standard environmental conditions as detailed in [58]. The satellite receiving telescope is modeled with an aperture diameter of 150 cm, representing a high-performance optical payload. Note that

the size can range from 30 cm to 2 m [59, 61–63]. To balance the minimization of atmospheric scattering with the spectral response of commercial photodetectors, the operating wavelength is set to $\lambda = 800$ nm, where the detector efficiency is approximately $\eta_{det} \approx 0.6$ [58]. The total measurement efficiency of the onboard optical setup is estimated at $\eta_{meas} = 0.25$. This value accounts for the cumulative losses from two polarizing beam splitters (transmissivity ~ 0.91 each) [58], the detector efficiency, and the intrinsic 50% limit of linear optical Bell state measurements (modeled as a 0.5 efficiency factor for the $45°$ wave-plate). Regarding environmental noise, we assume an average Earth surface temperature of 27°C (300 K). Finally, recognizing that precise timing is critical for mode matching, we adopt a conservative value of $\Delta t_{sync} = 3$ ns for the clock synchronization precision between the ground stations and the satellite, although recent experiments suggest precisions below 1 ns are achievable [60]. All other parameters are specified in [58].

6.2.3 Numerical Results and Discussion

In this section, we present the numerical results obtained from the simulation framework described previously (see Appendix B). The analysis focuses on the trade-offs between the geometric configuration of the satellite link (altitude, ground separation) and the temporal parameters of the photon generation (pulse width, gating window). The primary metrics of interest are the Practical Fidelity (F) and the Overall Success Probability (η_{tot}).

6.2.3.1 Impact of Link Geometry

First, we examine how the satellite's position relative to the ground stations affects the link performance. We fix the pulse width at $\sigma_t = 10$ ns and the gating window at $t_{gate} = 40$ ns, varying the satellite altitude h from 200 km to 1000 km for different ground separations D_G.

Fidelity vs. Altitude

Figure 6.5 illustrates the behavior of Fidelity as a function of altitude.

We observe distinct behaviors depending on the ground separation distance.

- For short separations ($D_G = 300$ km, blue line), the fidelity peaks at lower altitudes and monotonically decreases as the satellite rises. This is because the signal path is relatively short, so maximizing atmospheric transmittance at low zenith angles is the priority.
- For larger separations ($D_G \geq 1200$ km, green and red lines), we observe a characteristic "hump" where fidelity initially increases up to an altitude of ≈ 400 km before declining. This is explained by the interplay between atmospheric turbulence and free-space loss. At very low altitudes ($<$ 300 km), the satellite appears near the horizon (large zenith angle), forcing the beam through a thicker turbulent air mass. As the altitude increases, the zenith angle improves, increasing fidelity. However, beyond a certain point, the geometric beam widening due to the increased slant range dominates, reducing the SNR and Fidelity.

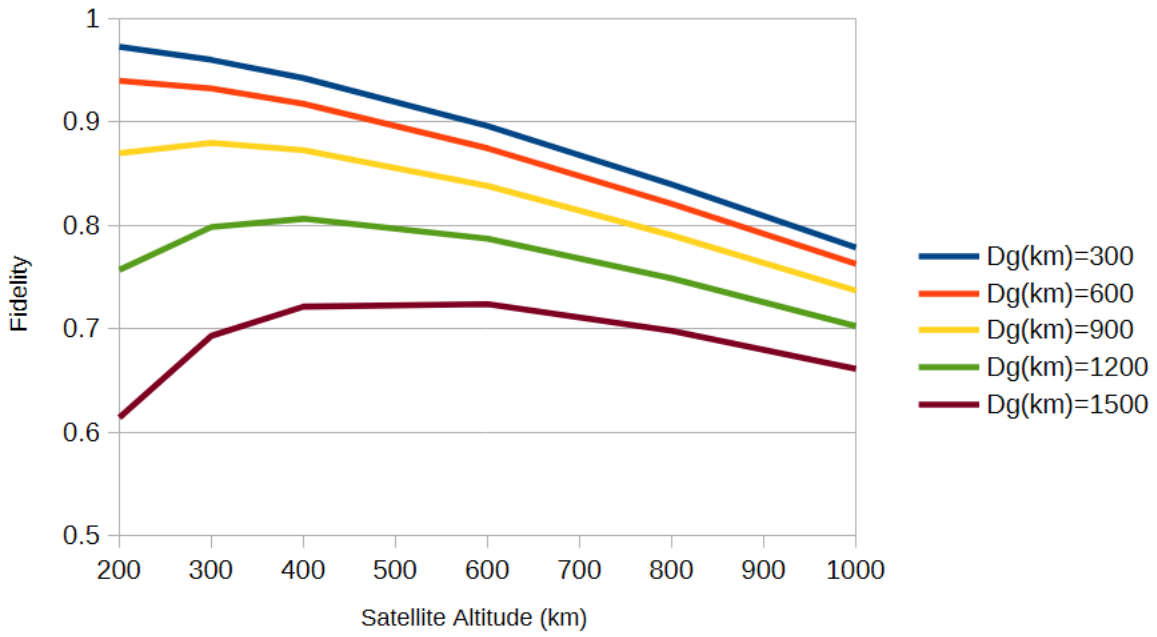

Figure 6.5: Practical Fidelity (F) as a function of Satellite Altitude (h) for various ground station separations (D_G). Parameters: $\sigma_t = 10$ ns, $t_{gate} = 40$ ns.

Success Probability vs. Altitude

Figures 6.6 and 6.7 display the Overall Success Probability (η_{tot}) in two different scales to highlight the rapid decay.

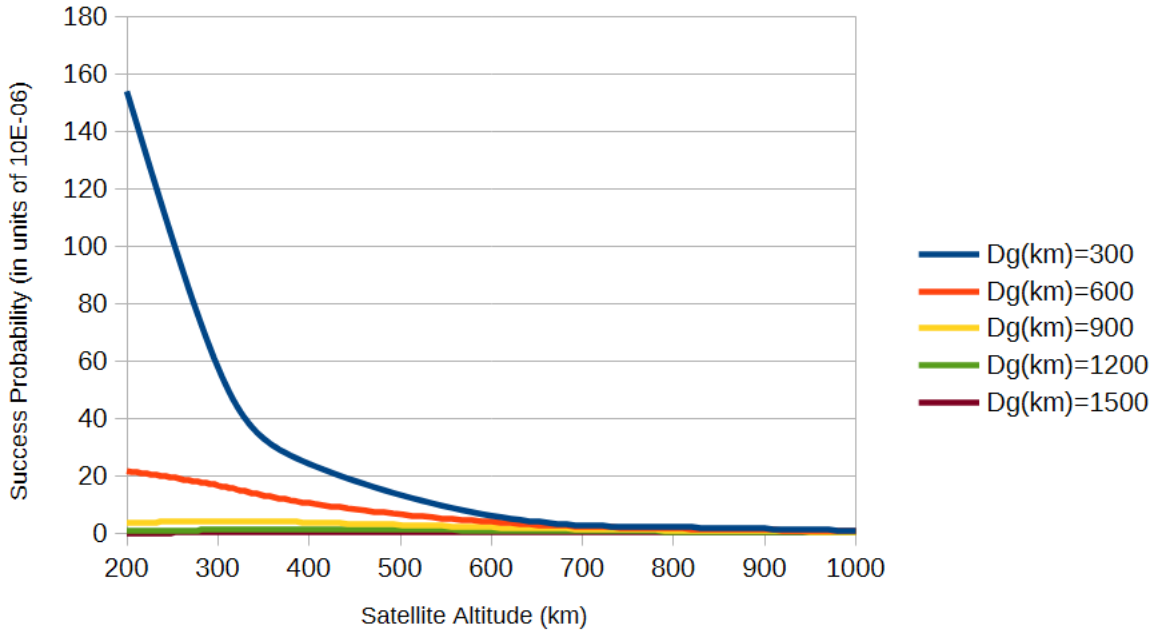

Figure 6.6: Overall Success Probability (η_{tot}) versus Satellite Altitude (Full Scale). The probability decays exponentially with distance. Parameters: $\sigma_t = 10$ ns, $t_{gate} = 40$ ns.

The success probability follows a strict decay curve driven by beam widening. For a baseline of $D_G =$

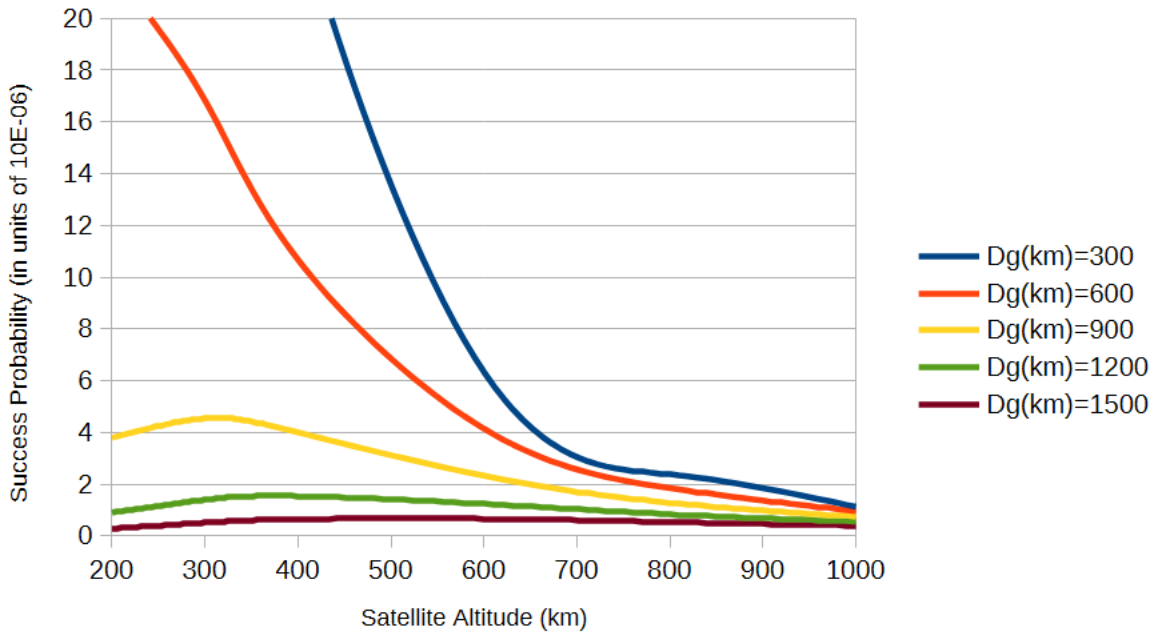

Figure 6.7: Zoomed-in view of the Success Probability for lower probabilities, highlighting the performance at larger ground separations ($D_G \geq 900$ km). Parameters: $\sigma_t = 10$ ns, $t_{gate} = 40$ ns.

300 km at 200 km altitude, we achieve relatively high efficiency ($\sim 1.5 \times 10^{-4}$). However, as shown in Fig. 6.7, for larger separations (1500 km), the probability drops below 10^{-6}. This confirms that geometric loss is the dominant impairment in the uplink channel, as increasing the ground separation significantly extends the photon travel path.

6.2.3.2 Impact of Temporal Parameters

Next, we analyze the effect of synchronization and detection timing. We fix the satellite altitude at 500 km and the ground separation at 1000 km, varying the gating window size (t_{gate}).

Fidelity vs. Gating Window

Figure 6.8 demonstrates the critical trade-off between collecting the signal and rejecting the noise.

As the gating window widens, the fidelity decreases for all pulse widths.

- Noise Admission: The background noise accumulates linearly with time. Since the signal is temporally localized (Gaussian), opening the window beyond the pulse duration ($\approx 3\sigma_t$) adds only stray photons and dark counts, drastically reducing the Signal-to-Noise Ratio (SNR).
- Pulse Width Effect: Shorter pulses ($\sigma_t = 10$ ns, blue line) achieve higher maximum fidelity because they allow for narrower gating windows, effectively "filtering out" more temporal noise compared to longer pulses ($\sigma_t = 40$ ns, green line). Increasing the wave packet width decreases the fraction of the packet captured by a fixed window, leading to lower fidelity.

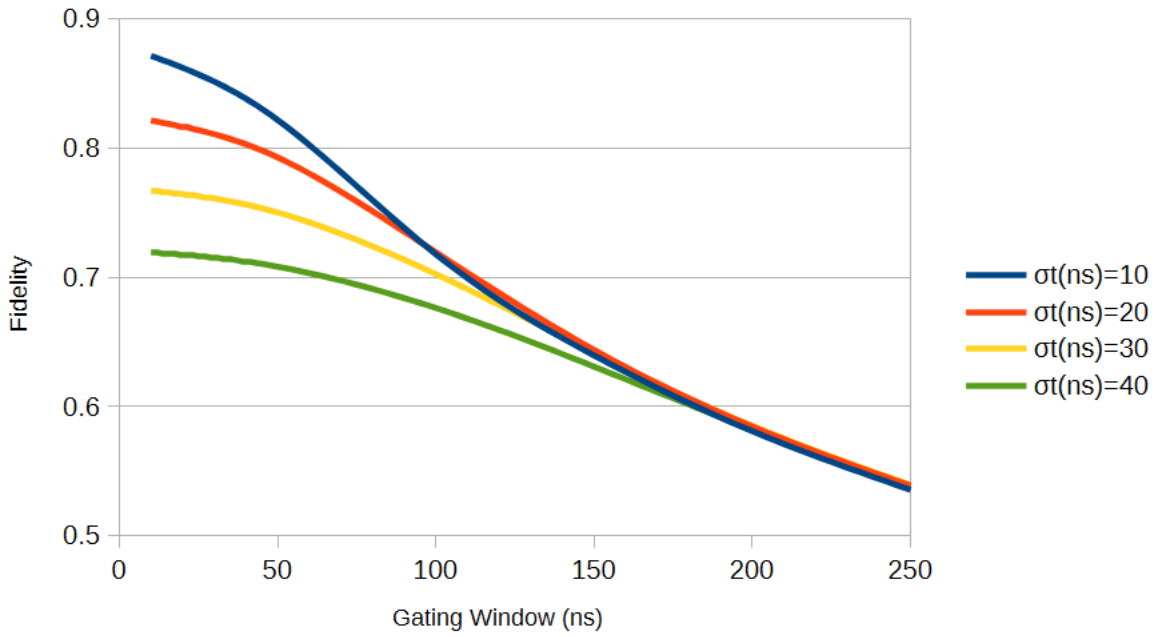

Figure 6.8: Practical Fidelity vs. Gating Window (t_{gate}) for different photon pulse widths (σ_t). Wider windows admit more noise, degrading fidelity. Parameters: $h = 500$ km, $D_G = 1000$ km.

Success Probability vs. Gating Window

Conversely, Figure 6.9 shows that the detection rate increases with the window size.

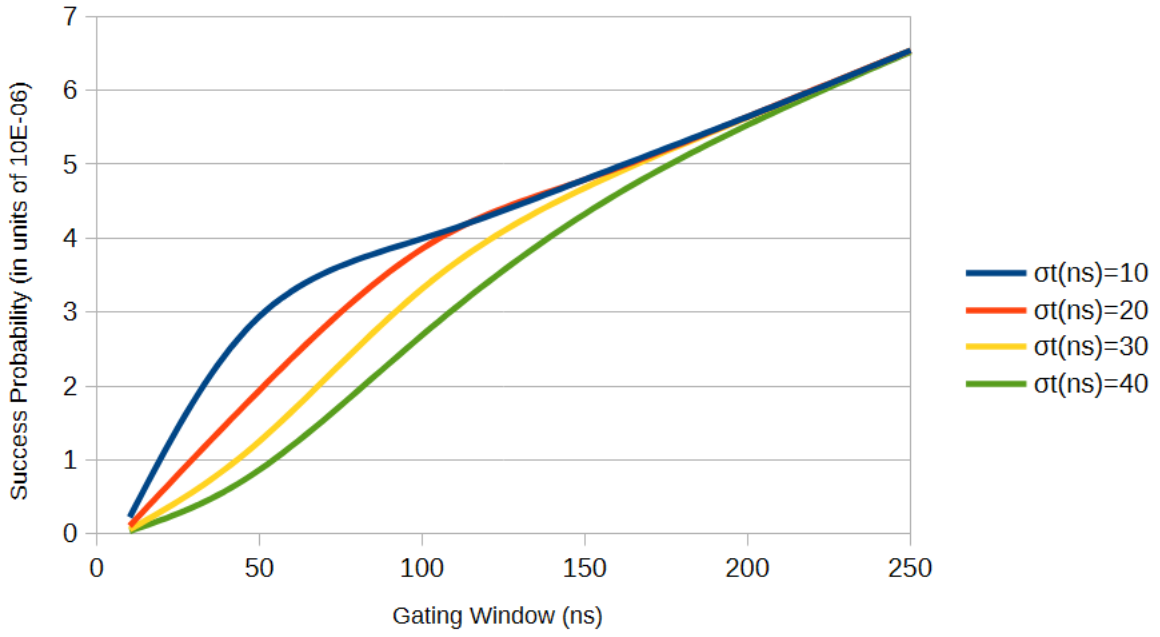

Figure 6.9: Success Probability vs. Gating Window. Wider windows capture more signal and noise, increasing the total detection rate. Parameters: $h = 500$ km, $D_G = 1000$ km.

Initially, the success probability rises rapidly as the window captures the main Gaussian peak of the photon. Beyond a certain point (> 100 ns), the increase becomes linear, driven purely by the accumulation

of background noise counts. Optimal operation requires selecting a window that captures the signal peak while minimizing the linear noise tail.

6.2.3.3 Feasibility Assessment

The simulation results indicate that uplink entanglement distribution is feasible under night-time conditions, provided that strict parameter bounds are met. The optimal configuration involves a low-Earth orbit ($h \approx 200 - 500$ km) and short baselines ($D_G < 600$ km), using short pulses ($\sigma_t \approx 10$ ns) and narrow gating windows (≈ 40 ns). In this regime, fidelities exceeding 0.9 are achievable with success probabilities on the order of 10^{-4} to 10^{-6}. These replicated results are compatible with the original results [46].

6.2.4 Architectural Assessment: Merits and Limitations

Based on the theoretical model and the numerical results presented above, we can critically assess the single-satellite dual uplink architecture. This configuration offers distinct logistical advantages but introduces severe physical constraints that limit its scalability.

6.2.4.1 Advantages

The primary strength of the uplink architecture lies in the asymmetry of resource allocation, shifting the technological burden from the orbiting satellite to the ground stations:

- **Reduced Satellite Complexity:** Since the photon sources and entanglement generation hardware are located on Earth, the satellite payload is reduced to a passive receiver consisting of simple linear optics (BSM) and detectors. This makes the satellite significantly lighter, cheaper to launch, and simpler to design compared to downlink sources.
- **Source Power and Flexibility:** Ground stations are not limited by the strict size, weight, and power (SWaP) constraints of a spacecraft. While a satellite is limited to roughly 10 kW of power , ground stations can utilize MW-scale power supplies [46]. This allows for high-intensity photon pumping to compensate for channel losses, as well as easy maintenance and upgrades of the quantum sources.

6.2.4.2 Disadvantages and Limitations

Despite the logistical benefits, the physics of the uplink channel imposes hard limits on performance:

- **Geometric Constraints (Simultaneous Visibility):** The most significant limitation is the requirement that the satellite must be visible to *both* ground stations simultaneously. As shown in our results (Fig. 6.7), this restricts the effective ground separation (D_G). For continental-scale distances (> 1200 km), the satellite must be at a very high altitude to be mutually visible, which in turn increases the path loss, rendering the link feasible only for regional networks.

- **Enhanced Atmospheric Loss (Shower Curtain Effect):** Unlike downlink, where the beam traverses the vacuum before hitting the atmosphere, in uplink, the beam encounters turbulence immediately at the transmitter. This results in severe beam wandering and widening at the receiver.
- **Synchronization Requirements:** The protocol relies on the interference of two independent photons at the satellite. This necessitates extremely precise clock synchronization (on the order of nanoseconds) and trajectory prediction to ensure the wavepackets overlap temporally.

In conclusion, the single-satellite uplink architecture is a viable solution for Metropolitan or Regional Area Quantum Networks, offering a cost-effective space segment. However, for intercontinental entanglement distribution, the geometric constraints suggest that multi-satellite or hybrid architectures may be required.

6.3 Dual-Satellite Dual Uplink Network

6.3.1 Architectural Design

The network consists of four primary nodes:

- Ground station Alice (A)
- Ground station Bob (B)
- Satellite S_A in view of Alice.
- Satellite S_B in view of Bob

The objective is to establish an entangled qubit pair between Alice and Bob by employing the entanglement swapping protocol.

Step 1: Entangled qubit pair generation

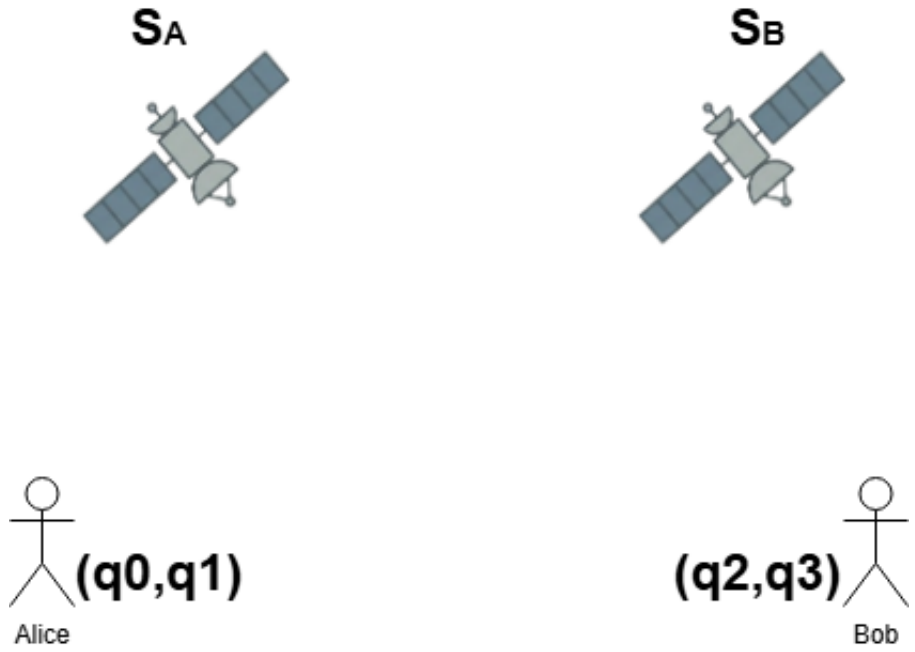

Figure 6.10: Both Alice and Bob generate an entangled qubit pair

Alice and Bob each generate an entangled qubit pair. Without loss of generality, let us assume that the pairs are generated in the Bell state $|\Phi^+\rangle$.

Step 2: Qubit transfer to satellite S_A

Qubit q_1 is transmitted from ground station Alice to satellite S_A.

Step 3: Qubit transfer to satellite S_B

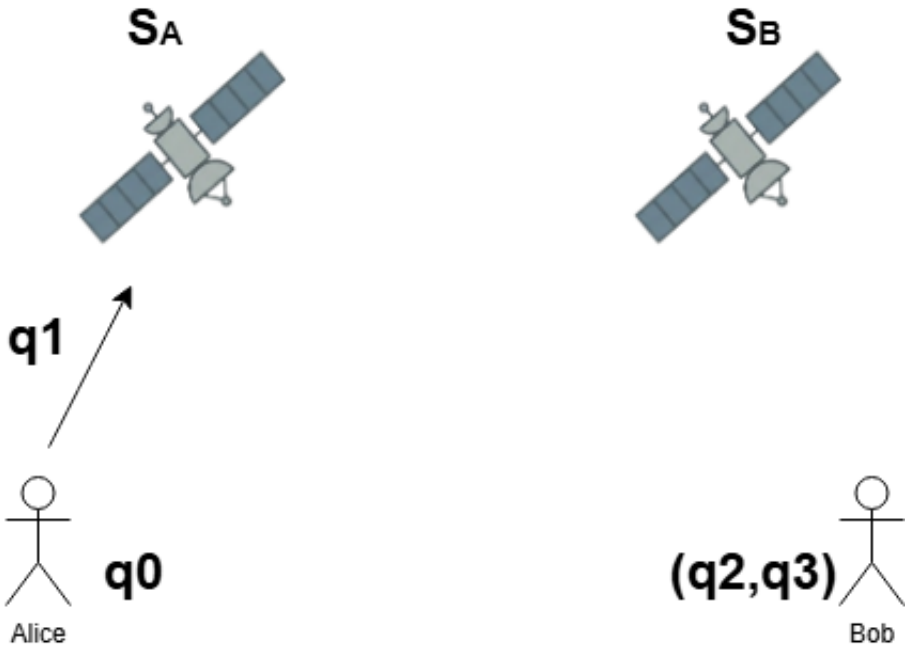

Figure 6.11: Alice sends qubit q_1 to S_A

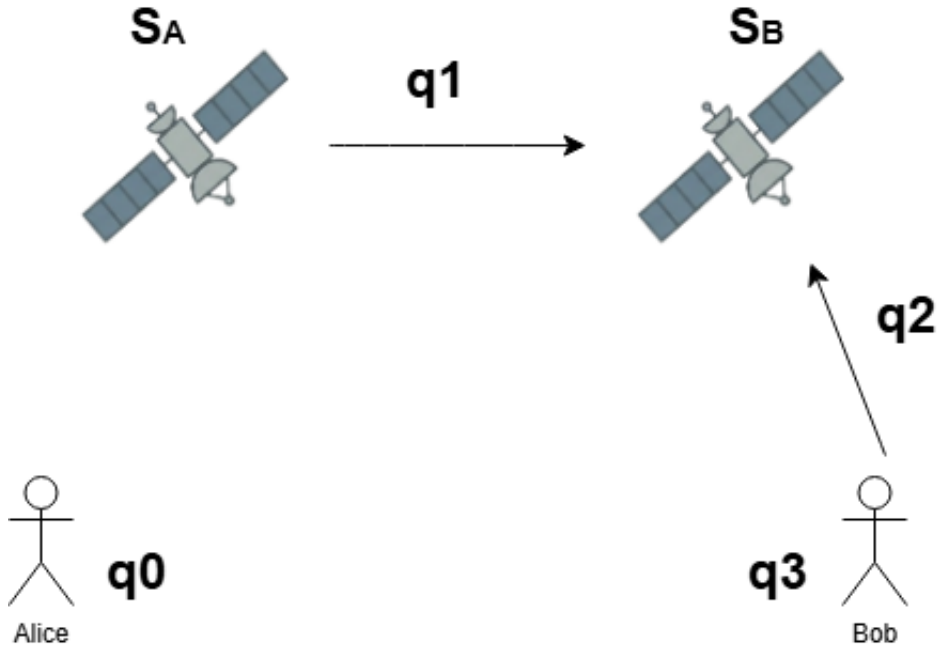

Figure 6.12: Qubits q_1 and q_2 are transferred to satellite S_B

Qubit q_1 is transferred from S_A to S_B and qubit q_2 is transferred from Bob to S_B. Note that the two qubits must reach the satellite at the same time.

Step 4: A BSM is performed by satellite S_B

Upon measurement, the state of the system collapses. Crucially, the remaining qubits q_0 and q_3 at the ground stations become entangled in a state that corresponds to the BSM outcome, as we have seen

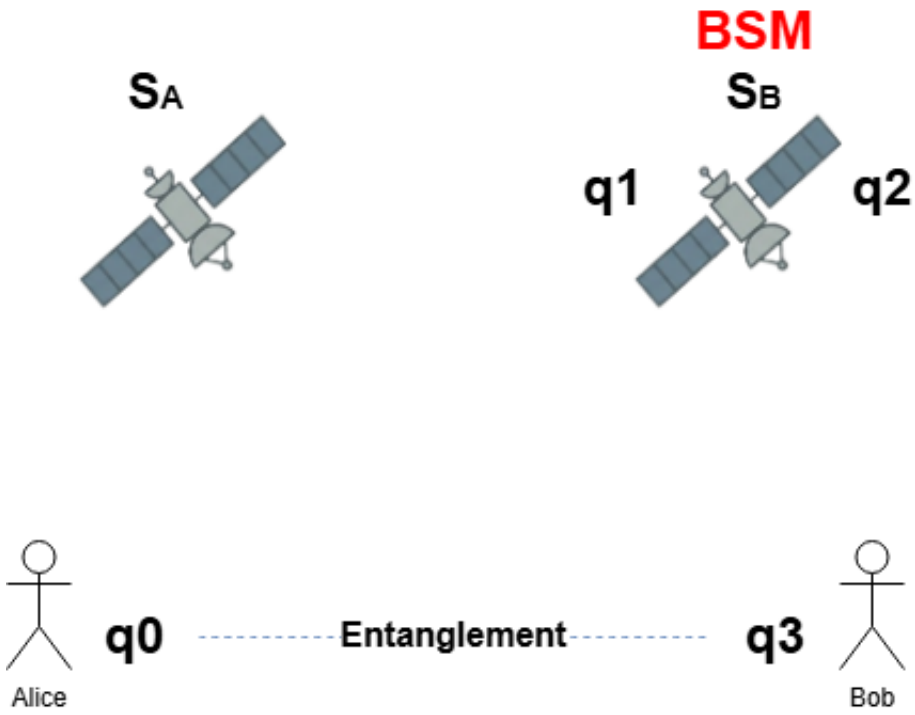

Figure 6.13: S_B performs a BSM

previously (6.2).

Step 5: Local correction

Satellite S_B informs Bob via a classical channel of the measurement result and Bob applies the appropriate local correction gates to transform the entangled state to the desired one.

6.3.2 Feasibility Analysis under Realistic Conditions

We now proceed to evaluate the dual-satellite architecture under realistic operating conditions. Our methodology builds upon the analysis developed for the single-satellite network [46], extending it to the dual-satellite topology while preserving a common basis for direct comparison. Before presenting the numerical results regarding success probability and fidelity, we qualitatively evaluate the fundamental differences between the two architectures.

6.3.2.1 Comparative Loss Analysis: Single-Satellite vs. Dual-Satellite Architecture

The fundamental structural distinction between the two networks lies in the network topology and the number of orbital nodes. The deployment of a dedicated satellite for each ground station introduces a critical degree of freedom: the decoupling of the ground distance (D_G) from the uplink geometry.

In the single-satellite case, increasing D_G forces the ground stations to point at low elevation angles, exponentially increasing atmospheric attenuation. In contrast, the dual-satellite architecture allows each

ground station to communicate with its local satellite near the zenith, regardless of the total distance D_G. This minimization of the atmospheric path length significantly reduces uplink losses. Furthermore, this topology enables viable quantum communication over intercontinental distances ($D_G > 1500$ km), a feat physically impossible with a single low-earth orbit (LEO) node due to the Earth's curvature.

This advantage comes at the cost of introducing an Inter-Satellite Link (ISL). While propagation in the vacuum of space eliminates atmospheric turbulence and beam wandering, the signal is still subject to free-space diffraction losses (beam widening). To mitigate this, our analysis assumes a transmitter with a larger beam waist radius compared to the ground stations. It is important to note that increasing the aperture in the single-satellite scenario would yield diminishing returns due to the dominant turbulent effects of the atmosphere. However, in the vacuum of the ISL, larger optics translate directly to higher link efficiency.

Note that mirror reflections do not inherently degrade photonic entanglement. In practical satellite systems, optical elements are macroscopic and effectively immovable, so the interaction between a photon and a mirror applies a deterministic transformation without introducing significant uncertainty. As long as the reflection is polarization-independent, entanglement encoded in polarization is preserved. Any potential entanglement degradation due to mirror recoil or polarization-dependent effects is negligible compared to dominant loss and decoherence mechanisms in satellite links.

6.3.2.2 Engineering Challenges

The transition to a dual-node architecture introduces two major engineering challenges that must be addressed:

1. **Temporal Synchronization (Mode-Matching):** In the single-satellite architecture, the symmetric uplink paths simplify the simultaneous arrival of photons. In the dual-satellite case, the path lengths are asymmetric. Ground Station A must transmit its qubit significantly earlier than Ground Station B to compensate for the additional transit time across the ISL. Precise timing control is required to ensure that the photon from path 1 (Ground A $\rightarrow S_A \rightarrow S_B$) and the photon from path 2 (Ground B $\rightarrow S_B$) arrive at the Bell State Measurement (BSM) module on satellite S_B within the coherence time window.

2. **Point-Ahead Mechanism:** Due to the finite speed of light and the high orbital velocity of the satellites ($\approx$ 7.6 km/s), the receiving satellite (S_B) will have displaced significantly during the signal's transit time from S_A. Therefore, S_A cannot simply point at the instantaneous position of S_B but must implement a Point-Ahead Angle (PAA) mechanism to target the future position of the receiver with microradian precision.

6.3.2.3 Fixed Parameters

To reflect the realistic constraints of this architecture, specific simulation parameters have been adjusted:

- **Zenith Angle (θ):** We assume a fixed zenith angle for the uplinks. While a theoretical best-case scenario would imply $\theta = 0$ rad (zenith pass), we adopt a conservative approach of $\theta = 0.3$ rad ($\approx 17.2°$). This accounts for realistic orbital passes where the satellite may not be directly overhead, providing a robust lower bound for performance.
- **Beam Waist (w_0):** We assume an initial beam waist radius of $w_0 = 13$ cm [43, 64].
- **Spatial Jitter:** Finally, to account for the increased complexity of synchronizing two independent moving nodes, we assume an increased spatial jitter of 5 ns (approx. 1.5 m path mismatch).

All other parameters and assumptions are similar to the ones in the single-satellite network.

6.3.3 Numerical Results and Discussion

In this section, we present the numerical results derived from the simulations of the dual-satellite architecture (see Appendix C). The analysis focuses on two primary performance metrics: the overall success probability (η_{tot}) and the practical fidelity (F). For all subsequent simulations, we fix the photon pulse width at $\sigma_t = 10$ ns and the gating window at $t_{gate} = 40$ ns.

6.3.3.1 Performance at Regional Scales ($D_G \leq 1500$ km)

We begin by examining the system performance at shorter inter-ground station distances to provide a direct comparison between the single-satellite and dual-satellite architectures. The results for various ground station distances D_G are illustrated in Figures 6.14, 6.15 and 6.16.

The comparison of the single and dual-satellite architectures as a function of the ground station distance D_G for a satellite altitude of $h = 500$ km, is illustrated in Figures 6.17 and 6.18.

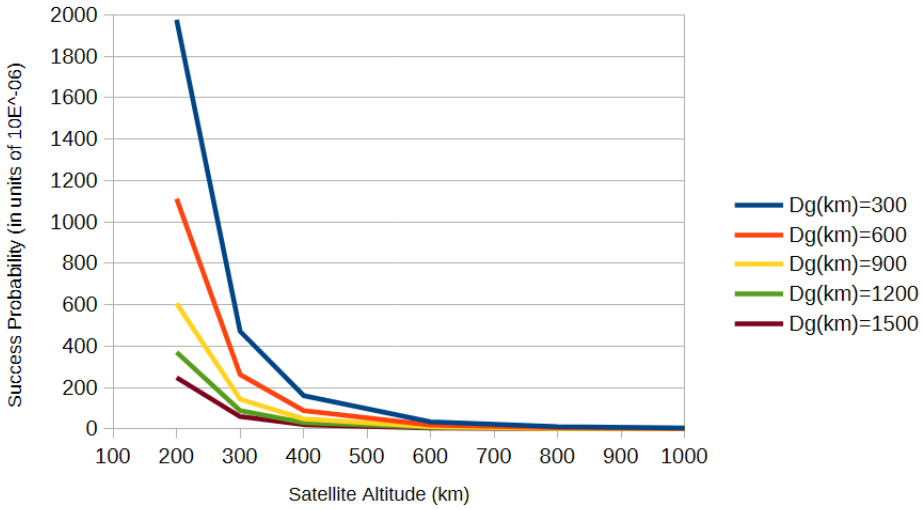

Figure 6.14: Success probability as a function of satellite altitude ($h \leq 1000$ km) for different ground station distances D_G.

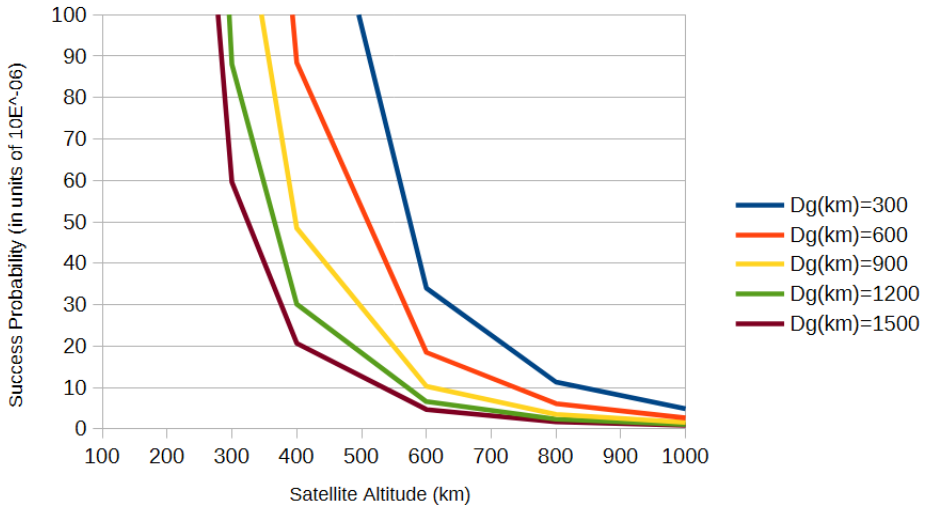

Figure 6.15: Success probability as a function of satellite altitude ($h \leq 1000$ km) for different ground station distances D_G (zoomed in).

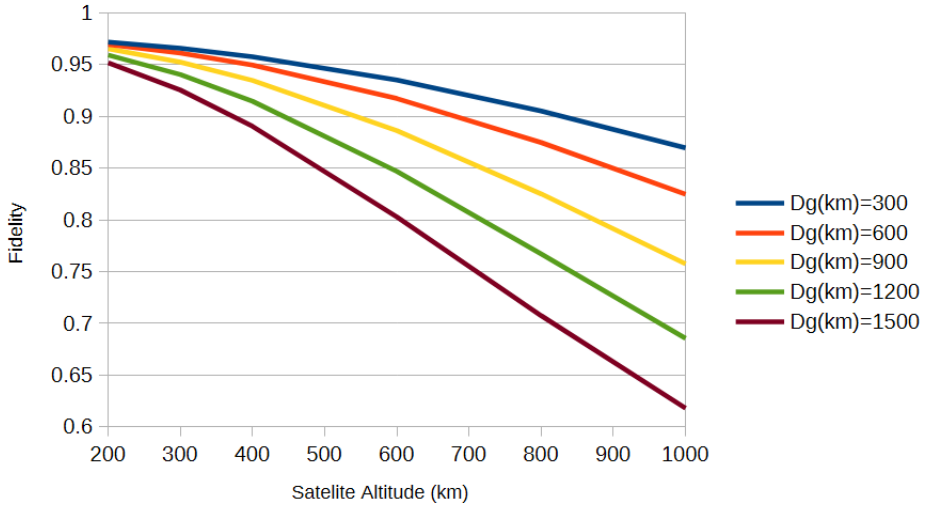

Figure 6.16: Fidelity as a function of satellite altitude ($h \leq 1000$ km) for different ground station distances D_G.

Overall Success Probability

As observed in Figure 6.14, the success probability exhibits an inverse relationship with the satellite altitude h. Lower orbits (e.g. $h = 500$ km) yield higher detection rates due to the minimized path length of the vertical uplinks.

Crucially, the dual-satellite architecture demonstrates a significant performance enhancement compared to the single-satellite baseline. For a specific case study at $h = 500$ km and $D_G = 500$ km (with identical optical parameters), the single-satellite architecture yields an overall success probability of approximately 3.34×10^{-5}, whereas the dual-satellite architecture achieves 4.67×10^{-5}. This increase is attributed to the optimal vertical geometry of the uplinks, which mitigates atmospheric attenuation.

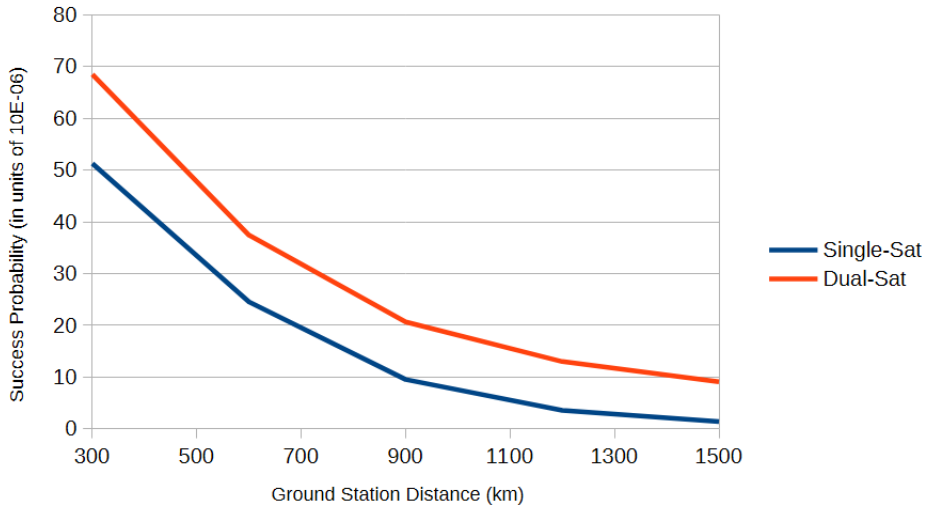

Figure 6.17: Comparison of the single and dual-satellite architectures' success probability as a function of ground station distance ($D_G \leq 1500$ km) for $h = 500$ km.

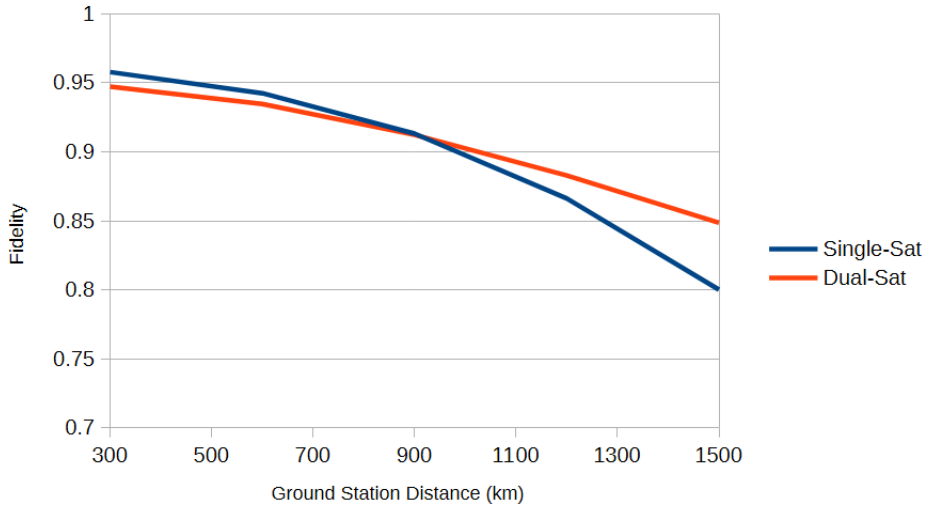

Figure 6.18: Comparison of the single and dual-satellite architectures' fidelity as a function of ground station distance ($D_G \leq 1500$ km) for $h = 500$ km.

Fidelity

As observed in Figure 6.16, for $h = 500$ km, the fidelity remains remarkably robust, initiating at $F \approx 0.95$ and maintaining values above 0.90 for $D_G \leq 900$ km. Conversely, at $h = 1000$ km, the increased diffraction losses significantly weaken the signal, causing the fidelity to drop toward 0.75.

The fidelity results for smaller distances for the dual-satellite topology are comparable to the single-satellite architecture. Revisiting the case study at $h = 500$ km and $D_G = 500$ km, the single-satellite architecture yields a fidelity of ≈ 0.937. whereas the dual-satellite topology yields a fidelity of ≈ 0.94.

6.3.3.2 Performance at Intercontinental Scales ($D_G \geq 1500$ km)

Subsequently, we extend the analysis to greater ground distances, showcasing the fundamental advantage of the dual-node topology: its ability to bridge distances physically inaccessible to a single LEO node. The results are presented in Figures 6.19 and 6.20.

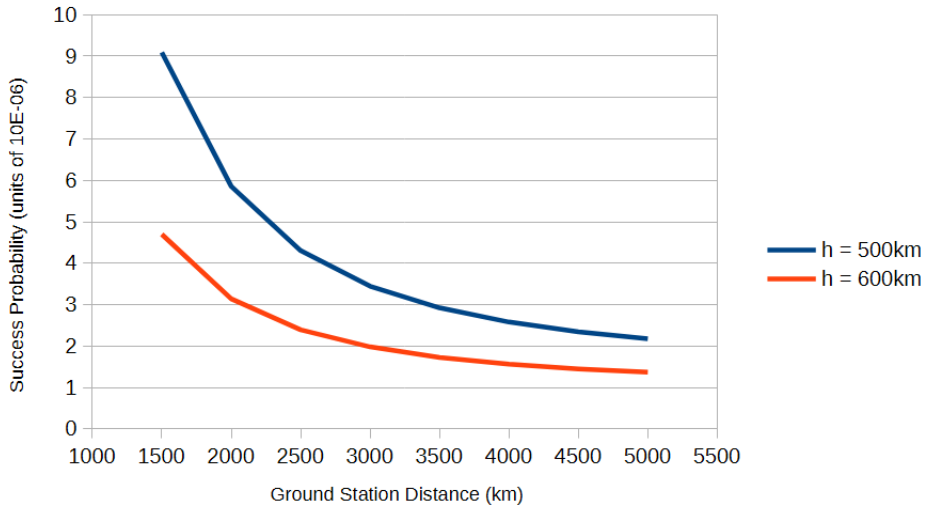

Figure 6.19: Success probability as a function of ground distance ($D_G \geq 1500$ km) for different satellite altitudes h.

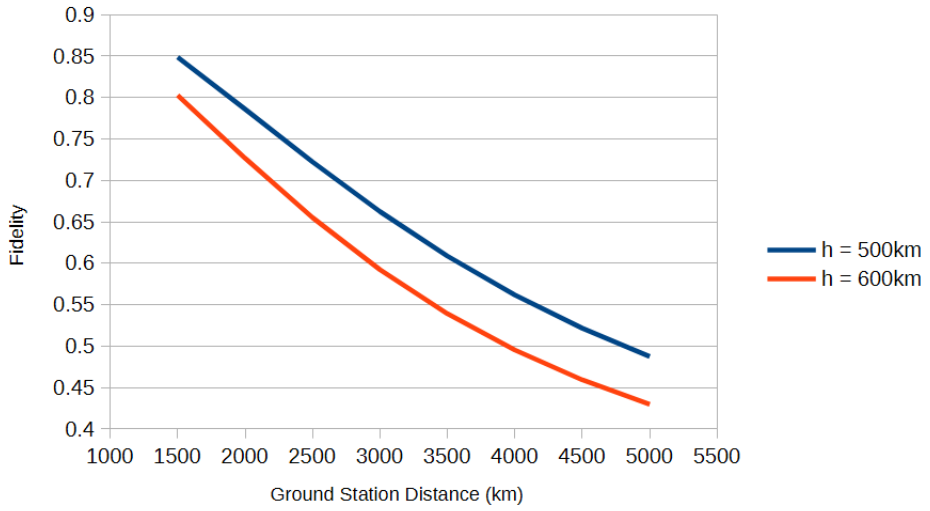

Figure 6.20: Fidelity as a function of ground distance ($D_G \geq 1500$ km) for different satellite altitudes h.

Overall Success Probability

The simulation results, observed in Figure 6.19, indicate that operational success probabilities in the order of 10^{-6} are achievable for satellite altitudes of 500-600 km, even at distances approaching 5000 km. It should be noted, however, that while the signal remains detectable at these ranges, the choice of altitude involves a trade-off: lower altitudes ($h = 500$ km) maximize the signal strength but impose a stricter geometric horizon limit (~ 5000 km), whereas slightly higher orbits ($h = 600$ km) provide a

safer geometric margin for intercontinental links at the cost of a marginal reduction in received flux.

Fidelity

The results in Figure 6.20, show that as the ground distance extends into the intercontinental regime, the structural advantage of the dual-node architecture becomes evident, albeit facing significant challenges at extreme ranges. The primary factor limiting fidelity at these ranges is the reduction in the SNR. As the distance between the two satellites increases, the beam divergence causes the spot size to exceed the receiver's aperture, resulting in a signal that gradually approaches the noise floor of the detectors (dark counts).

Specifically, for a satellite altitude of $h = 600$ km, the fidelity stands at $F \approx 0.80$ at 1500 km but degrades to $F \approx 0.43$ at 5000 km. Although the fidelity at 5000 km falls below the classical limit for secure communication, the dual-satellite architecture still outperforms the single-satellite configuration at intermediate intercontinental distances (e.g. at 2000 km, $F_{dual} \approx 0.73$ vs $F_{single} \approx 0.68$), while also maintaining significantly higher success probabilities. This confirms that the replacement of stochastic atmospheric losses with deterministic vacuum diffraction provides a more "graceful" degradation of the quantum state, extending the operational reach of the network.

6.3.4 Architectural Assessment: Merits and Limitations

6.3.4.1 Operational limits

Taking into account the results presented in the previous section, the dual-satellite architecture remains operational for distances up to around 2000 km. The Fidelity at this point, has reached a borderline acceptable 0.73 and the further increase of the distance results in unacceptable fidelity levels for secure communication. Note that, although the success probability at higher distances remains at operational values, the low fidelity results imply that the success probability results are attributed to noise and dark counts rather than to the actual signal.

However, this is still a major step forward compared to the single-satellite architecture and serves as the base for further improvements.

6.3.4.2 Advantages

- **Atmospheric Decoupling:** The most significant advantage is the decoupling of the total communication distance from atmospheric losses. Since the ground-to-satellite uplinks remain near-vertical ($\theta \approx 0.3$ rad), the atmospheric attenuation and turbulence-induced noise remain minimal and constant, regardless of whether the ground stations are separated by 100 km or 5000 km.

- **Intercontinental Operational Range:** This architecture enables viable quantum links over intercontinental distances ($D_G > 2000$ km). It effectively bypasses the geometric horizon limits and the exponential signal collapse that plagues single-satellite configurations at low elevation angles.

- **Deterministic Loss Profile in Vacuum:** Unlike the stochastic nature of atmospheric turbulence in the single-satellite architecture, the ISL segment in the dual-satellite architecture operates in a vacuum. The losses are purely deterministic, governed by Gaussian beam diffraction ($\propto 1/L^2$), allowing for more predictable system performance and stable Signal-to-Noise Ratios (SNR).

- **Superior Transmission Rates:** Due to the reduced total path loss at long distances, the dual-satellite architecture maintains a success probability in the order of 10^{-6}, which is nearly an order of magnitude higher than the 10^{-7} range observed in the single-satellite architecture for the same distances.

6.3.4.3 Disadvantages

- **Hardware and Structural Complexity:** The dual-satellite architecture requires double the number of orbital nodes and significantly more complex payloads. Each satellite must be equipped with multiple optical terminals to manage simultaneous ground-to-space and space-to-space links.

- **Stringent Temporal Synchronization:** Achieving the necessary temporal mode-matching for Bell State Measurements (BSM) is highly challenging. The assumed 5 ns jitter requires sub-nanosecond precision in clock synchronization between two independent, high-velocity orbital nodes.

- **Orbital Dynamics and Point-Ahead Angle (PAA):** Targeting a laser beam between two satellites traveling at $\sim$ 7.6 km/s requires microradian pointing precision. A sophisticated Point-Ahead Angle mechanism is mandatory to compensate for the displacement of the receiver during the photon's time-of-flight.

- **Vacuum Diffraction Limits:** While vacuum propagation avoids turbulence, beam divergence (widening) remains a limiting factor.

6.3.4.4 Comparative Summary

To synthesize the findings, table 6.4 summarizes the operational trade-offs between the two architectures based on our simulation results.

Table 6.4: Operational Comparison between Single-Satellite and Dual-Satellite Architectures.

Metric	Single-Satellite Architecture	Dual-Satellite Architecture
Optimal Coverage Range	0 – 1000 km	0 – 1800 km
Operational Limit	$\approx$ 1200 km	$\approx$ 2200 km
Success Prob. ($D_G = 2000$ km)	$\sim 10^{-7}$	$\sim 10^{-6}$
Fidelity ($D_G = 2000$ km)	~ 0.68 (Insecure)	~ 0.73 (Marginal)
Engineering Complexity	Low (1 Sat)	High (2 Sats + ISL Sync)

6.3.4.5 Possible Improvements and Future Directives

While the current simulation demonstrates the feasibility of the dual-satellite architecture under conservative assumptions, several technical optimizations could further extend its operational range.

Expansion of the Initial Beam Waist

The primary limiting factor in the Inter-Satellite Link (ISL) is Gaussian beam diffraction. According to the far-field divergence relation, $\theta_{div} \cong \lambda/(\pi w_0)$, increasing the initial beam waist w_0 results in a more collimated beam.

- **Impact:** Transitioning to a larger beam waist would increase the Rayleigh range, ensuring that a larger fraction of the photon flux is captured by the receiver's aperture at distances of 5000 km.
- **Trade-off:** This requires larger and heavier optical telescopes (Size, Weight, and Power - SWaP constraints), necessitating a more robust satellite bus.

Optimization of Constellation Density for Lower Zenith Angles (θ)

The current analysis assumed a conservative zenith angle of $\theta = 0.3$ rad. Minimizing this angle reduces the effective air mass ($AM \approx \sec\theta$) the signal must traverse.

- **Strategy:** By increasing the number of satellites in the LEO constellation (higher orbital density), the probability of a satellite being positioned directly above a ground station (Zenith pass, $\theta \to 0$) increases.
- **Benefit:** This would virtually eliminate atmospheric turbulence effects and maximize the uplink efficiency, providing a higher baseline signal before it enters the ISL segment.

Advanced Mode-Matching and Jitter Reduction

The quantum interference required for Bell State Measurements (BSM) relies on the indistinguishability of the arriving photons.

- **Temporal Synchronization:** Improving the synchronization of the onboard atomic clocks and using sub-nanosecond pulse-position modulation could reduce the spatial jitter from 5 ns to the picosecond regime.
- **Spatial Mode-Matching:** Implementation of onboard Adaptive Optics (AO) could correct wavefront distortions in real-time, ensuring that the spatial overlap of the two photons at the beam splitter is near-perfect, thereby pushing the fidelity closer to the theoretical limit of 1.0.

Integration of Quantum Repeaters

In the long term, the most transformative improvement would be the transition from a passive relay to an active Quantum Repeater node.

- **Mechanism:** By incorporating quantum memories and entanglement swapping protocols, the architecture would no longer be limited by the direct transmission loss of photons. Instead, the loss would scale linearly rather than exponentially, enabling ultra-secure, high-fidelity communication over arbitrary global distances.

6.3.5 Scalability: Expansion to n-Satellite Relay Chains

The dual-satellite architecture analyzed in this work serves as the fundamental building block for a scalable, global-scale quantum constellation. Extending this model to a chain of n satellites (multi-hop relay) represents the next logical step toward a permanent quantum backbone.

Gains and Opportunities

- **Global Coverage:** An n-satellite chain removes all remaining geographical constraints, enabling entanglement distribution between any two points on Earth, regardless of the terrestrial distance.
- **Hop-Distance Optimization:** In an n-node chain, the distance of each individual Inter-Satellite Link (ISL) can be reduced. By keeping each segment shorter, the geometric diffraction losses per hop are minimized, potentially allowing for the use of smaller, more cost-effective optical apertures.
- **Network Resilience:** A multi-node constellation offers routing flexibility. If one satellite node is unavailable (e.g. due to technical failure or solar interference), the quantum information can be rerouted through alternative orbital paths.

Technical Challenges

- **Compounded Transmission Losses:** In a passive relay configuration, the total success probability scales multiplicatively with the number of hops ($\eta_{tot} \propto \eta_{ISL}^{n-1}$). Without the use of active quantum repeaters to "refresh" the signal, the photon count at the final destination would diminish exponentially, eventually falling below the noise floor.
- **Multi-Node Temporal Synchronization:** The complexity of mode-matching grows exponentially with n. Coordinating the simultaneous arrival of wavepackets from n independent platforms—each subject to distinct orbital perturbations and relativistic effects—requires a revolutionary leap in distributed space-based timing.
- **Hardware Overhead:** Each intermediate node must function as a high-speed quantum "switch", capable of performing multiple Bell State Measurements (BSM) or maintaining entanglement swapping protocols in real-time.

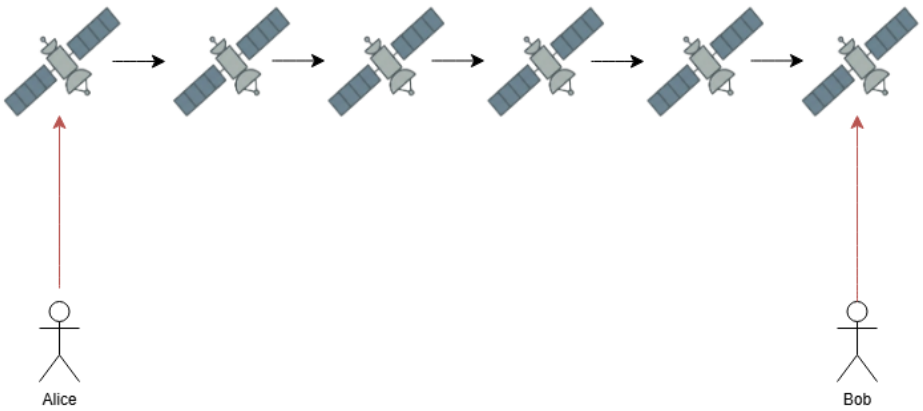

Figure 6.21: Overview of the generalized n-satellite network.

6.4 Single-Satellite Hybrid Uplink-Downlink Network

6.4.1 Architectural Design

The network consists of three primary nodes:

- Ground station Alice (A)
- Ground station Bob (B)
- A single satellite in common view of both ground stations

Step 1: Entangled qubit pair generation

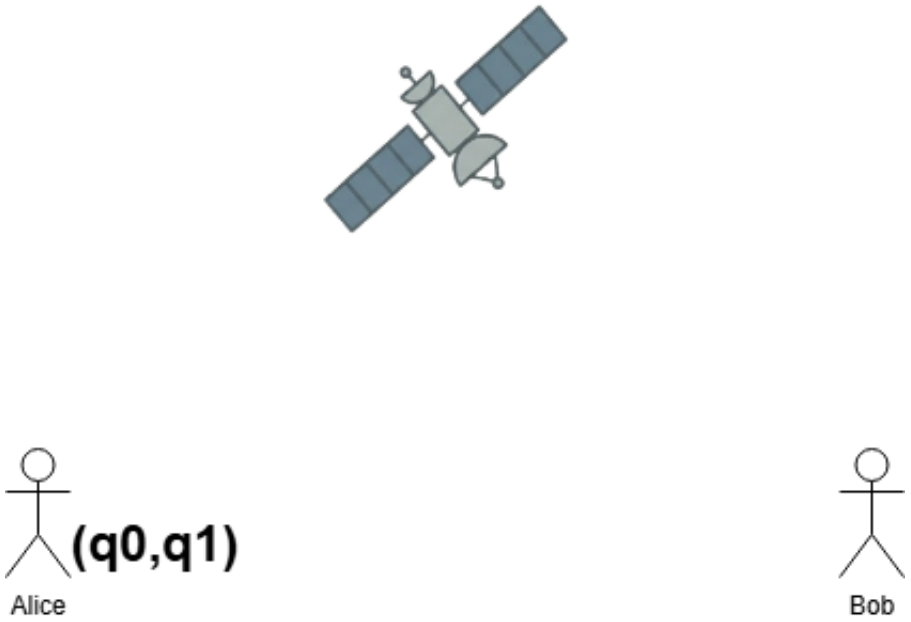

Figure 6.22: Alice generates an entangled qubit pair

Alice generates an entangled qubit pair in the Bell state $|\Phi^+\rangle$

Step 2: Uplink qubit transfer to the satellite

Qubit q_1 is transmitted from ground station Alice to the satellite.

Step 3: Downlink qubit transfer to Bob

Qubit q_1 is transferred from the satellite to Bob. Alice and Bob now each possess a qubit of the original entangled qubit pair.

6.4.2 Feasibility Analysis

The feasibility of the single-satellite hybrid relay is evaluated based on a fundamental shift in the operational principles compared to the dual-uplink entanglement swapping schemes. The primary advantages

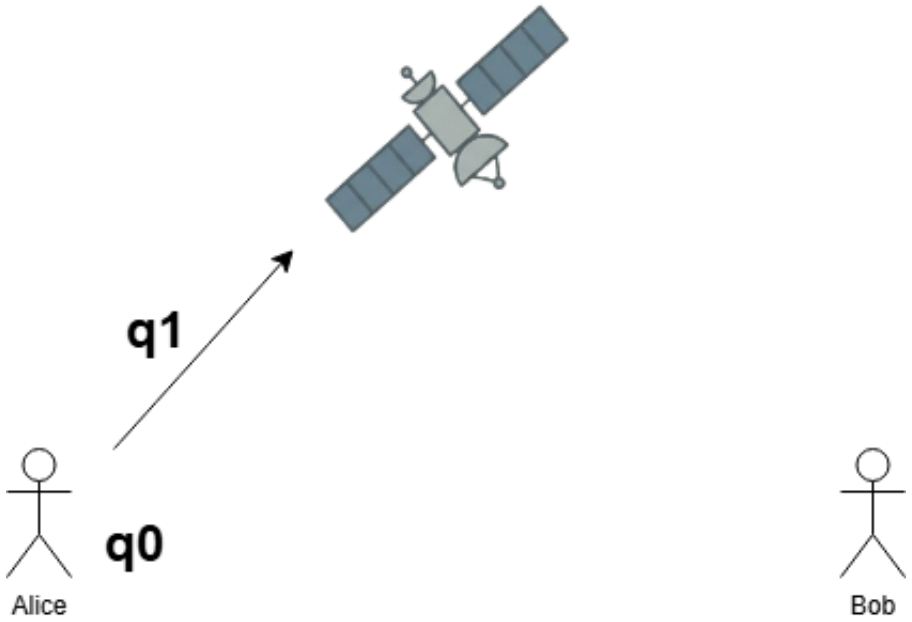

Figure 6.23: Alice sends qubit q_1 to the satellite

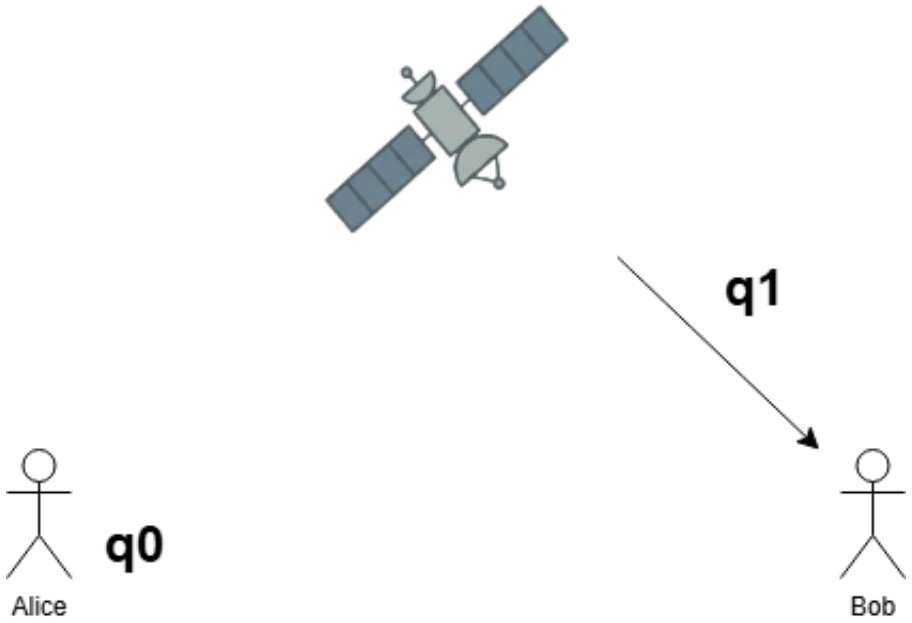

Figure 6.24: Qubit q_1 is transferred to Bob

that justify the hybrid approach are categorized below:

6.4.2.1 Probabilistic Scaling: Coincidence vs. Survival

In dual-uplink architectures, the end-to-end success probability (η_{tot}) is a **coincidence-based process**. It requires two independent, highly attenuated upward channels to succeed simultaneously within the

satellite's temporal window:

$$\eta_{dual} \approx (\eta_{up,A} \cdot \eta_{up,B}) \cdot P_{BSM} \tag{6.15}$$

where P_{BSM} is the Bell State Measurement efficiency ($\leq 50\%$ for linear optics). Conversely, the hybrid architecture operates as a **serial quantum channel**, where a single photon carrier must 'survive' a chain of events:

$$\eta_{hybrid} = \eta_{up} \cdot \eta_{relay} \cdot \eta_{down} \cdot \eta_{det} \tag{6.16}$$

where η_{relay} (Internal Relay Efficiency) represents the fixed optical losses within the satellite's internal hardware. It accounts for the photon's path through mirrors, filters, and lenses during re-routing. Unlike link losses, it remains constant regardless of distance. Since the downlink efficiency η_{down} is typically orders of magnitude higher than the uplink efficiency η_{up} [45, 65], hybrid architectures involving a single uplink and a single downlink transmission scale linearly with η_{up} rather than quadratically, thereby avoiding the severe suppression present in double-uplink entanglement swapping schemes.

6.4.2.2 Atmospheric Asymmetry and the Shower Curtain Effect

A critical feasibility factor is the physical asymmetry between the two link types. In the uplink segment, the beam encounters the high-density, turbulent layers of the atmosphere at the **beginning** of its propagation. This results in significant beam wandering.

In contrast, the downlink segment benefits from the **shower curtain effect**: the beam propagates through the vacuum of space first and only encounters atmospheric turbulence in the final few kilometers of its path. Consequently, the downlink beam propagation is largely diffraction-limited, resulting in a ground footprint on the order of a few meters to several meters [45, 63, 66], depending on the satellite altitude and transmit optics.

6.4.2.3 Operational Robustness and Synchronization

The feasibility of the dual uplink architectures is strictly limited by the requirement for **sub-nanosecond temporal synchronization** and precise **spatial mode-matching** at the satellite's beam splitter. For entanglement swapping to occur, the two arriving photons must be indistinguishable in all degrees of freedom (frequency, time, and polarization)..

The hybrid architecture eliminates the need for multi-photon interference at the satellite. The operational requirement is reduced to ensuring the single photon arrives within the Bob's detector gating window. This significantly lowers the complexity of the satellite payload, as it functions as a passive or active relay without the need for onboard BSM hardware or picosecond-level clock synchronization across thousands of kilometers.

6.4.2.4 Model Assumptions and Limitations

The numerical analysis presented in this work is based on a semi-analytical link-budget model designed to assess the feasibility and relative performance of satellite-assisted quantum communication architectures. The model captures the dominant physical effects governing free-space quantum optical links, while intentionally adopting simplifying assumptions in order to maintain analytical transparency and computational tractability.

Atmospheric Conditions

Clear-sky, nighttime conditions are assumed throughout the analysis. Atmospheric losses are modeled using a Beer–Lambert exponential extinction law with a single scale height, representing molecular absorption and scattering in the absence of clouds, aerosols, or weather-induced fluctuations. Turbulence effects are included only for the uplink segment, under the assumption of weak atmospheric turbulence, consistent with standard night-time propagation models.

Geometrical Configuration

The satellite is assumed to be in a circular Low Earth Orbit, and the ground-to-satellite geometry is modeled using an Earth-centered spherical approximation. The ground separation distance is assumed to be symmetric with respect to the satellite ground track, such that the satellite is approximately located above the midpoint between the communicating ground stations. This assumption allows for a simplified yet representative evaluation of slant-range and zenith-angle dependent effects.

Optical Beam Propagation

Beam propagation is modeled assuming Gaussian spatial modes. In the uplink direction, both diffraction and turbulence-induced beam spreading are included, while in the downlink direction only diffraction is considered, capturing the so-called *shower curtain effect*. Wavefront distortions, adaptive optics compensation, and higher-order turbulence effects are neglected. Pointing and tracking errors are modeled as Gaussian beam wander with a fixed root-mean-square displacement.

Receiver and Detection Model

Collection efficiency is estimated using a Gaussian overlap approximation between the received optical beam and the receiver aperture. Detector inefficiencies are included as a fixed multiplicative factor. Effects such as detector afterpulsing, dead time, timing jitter, polarization mismatch, and mode-dependent coupling losses are not explicitly modeled.

Noise and Fidelity Estimation Background noise and detector dark counts are incorporated through an aggregate noise rate, representing the combined contribution of stray photons and intrinsic detector noise under night-time operation. The impact of noise on entanglement quality is quantified using a conservative signal-to-noise-based fidelity estimator, which provides a lower-bound estimate of the achievable entanglement fidelity. A full quantum bit error rate (QBER) analysis, including basis mismatch and multi-photon contributions, is beyond the scope of the present model.

6.4.2.5 Fixed Parameters

To ensure numerical consistency and a rigorous comparative analysis with the previously discussed architectures, all shared environmental and photonic parameters are kept identical. For the Hybrid Relay configuration, the following two parameters are specifically introduced:

- **Ground Receiver Radius (R_{ground}):** The radius of Bob's ground-based telescope is set to 75 cm (0.75 m). This ensures absolute hardware parity with the satellite's collection aperture, allowing the analysis to isolate the performance gains derived from the relay geometry rather than differences in collection area.
- **Internal Relay Efficiency (η_{relay}):** This parameter accounts for the fixed optical losses (absorption and scattering) encountered during the photon's internal routing through the satellite's optical assembly, including mirrors and spectral filters. A value of 0.90 is adopted, representing a high-performance, space-qualified optical relay [66].

6.4.3 Numerical Results and Discussion

In this section, we evaluate the performance of the hybrid quantum relay architecture (see Appendix D). To maintain a rigorous comparative framework, the simulations utilize the same fundamental parameters as the previous models: a photon pulse width of $\sigma_t = 10$ ns and a detector gating window of $t_{gate} = 40$ ns. Hardware parity is ensured by fixing the receiver aperture radius at $R_A = 0.75$ m for both the satellite and the ground station (Bob). A key addition to this model is the internal relay efficiency, set at $\eta_{relay} = 0.90$ [66].

6.4.3.1 Performance at Regional Scales ($D_G \leq 1500$ km)

We first examine the system's efficiency and signal quality at satellite altitudes up to 1000 km. The results for various ground station distances D_G are illustrated in Figures 6.25, 6.26 and 6.27.

The comparison of the three architectures as a function of the ground station distance D_G for a satellite altitude of $h = 500$ km, is illustrated in Figures 6.28 and 6.29.

Overall Success Probability

As shown in Figure 6.25, the hybrid architecture demonstrates a significant leap in success probability compared to the dual-satellite configuration. For a case study at $h = 600$ km and $D_G = 1000$ km, the hybrid relay achieves a total efficiency of $\eta_{tot} \approx 1.16 \times 10^{-3}$, which is roughly two orders of magnitude higher than the dual-satellite baseline ($\sim 10^{-5}$).

This performance gap is primarily due to the Shower Curtain Effect inherent in the downlink segment. Unlike the dual-uplink model where both photons suffer from early-path turbulence spreading, the hybrid downlink encounters atmospheric turbulence only at the very end of its trajectory. This keeps the beam

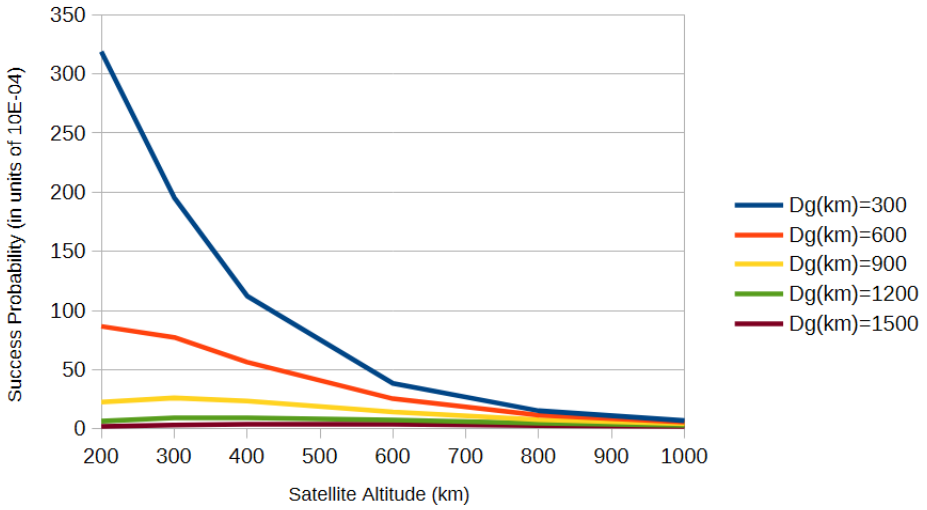

Figure 6.25: Success probability for the hybrid architecture ($h \leq 1000$ km) across different ground station distances D_G.

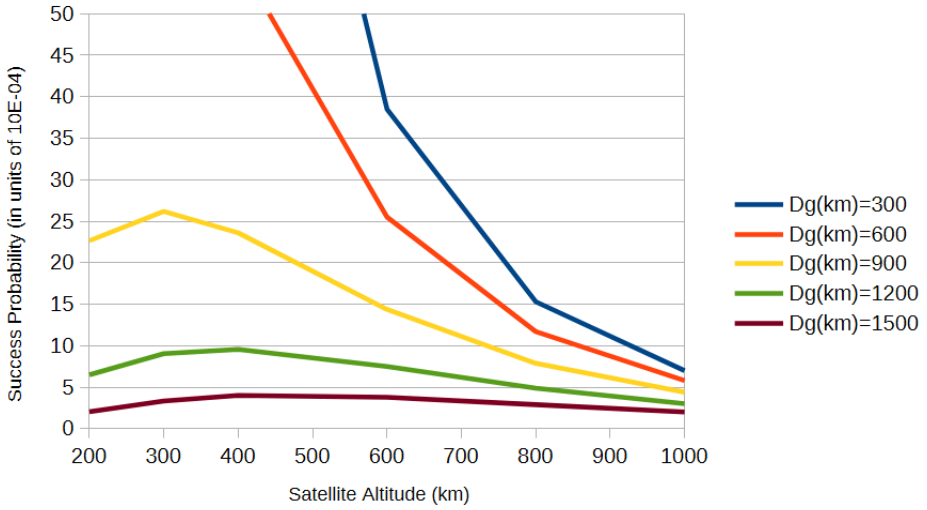

Figure 6.26: Success probability for the hybrid architecture ($h \leq 1000$ km) across different ground station distances D_G (zoomed in).

highly collimated for the majority of the link, allowing the 0.75 m aperture to collect the signal with near-optimal efficiency.

Fidelity

The fidelity results in Figure 6.27 highlight the most distinct advantage of the hybrid approach. For altitudes up to 700 km, the fidelity remains remarkably high, exceeding 0.95 throughout the 1000 km ground separation range.

The structural reason for this robustness is that the hybrid relay is purely SNR-limited. Unlike the dual uplink architecures, it is not affected by temporal synchronization jitter (x_0), as it does not rely on the simultaneous interference of two independent photons. As long as the collected signal remains signifi-

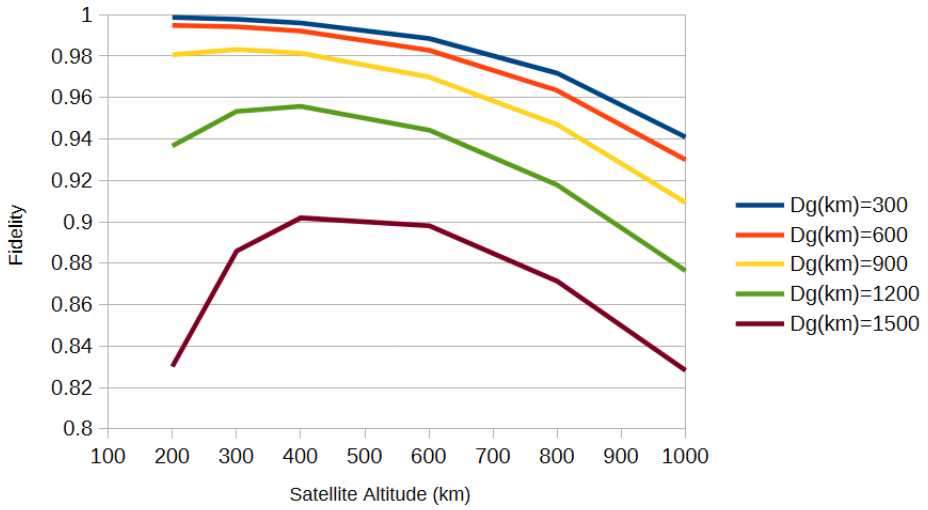

Figure 6.27: Fidelity for the hybrid architecture ($h \leq 1000$ km) across different ground station distances D_G.

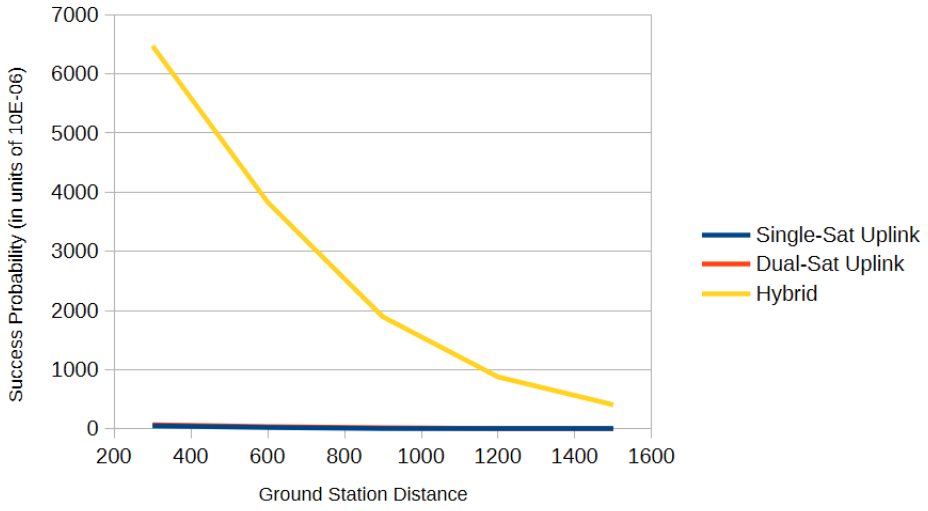

Figure 6.28: Comparison of the three architectures' success probability as a function of ground station distance ($D_G \leq 1500$ km) for $h = 500$ km.

cantly stronger than the background noise (1500 Hz), the fidelity remains near unity.

6.4.3.2 Performance at Intercontinental Scales ($D_G \geq 1500$ km)

To evaluate the scalability of the hybrid relay for global-scale quantum networking, the analysis is extended to ground distances ranging from 1500 km to 3000 km. This regime highlights the fundamental geometric limits of LEO-based links and the performance trade-offs associated with orbital altitude. The results are illustrated in Figures 6.30 and 6.31.

Overall Success Probability

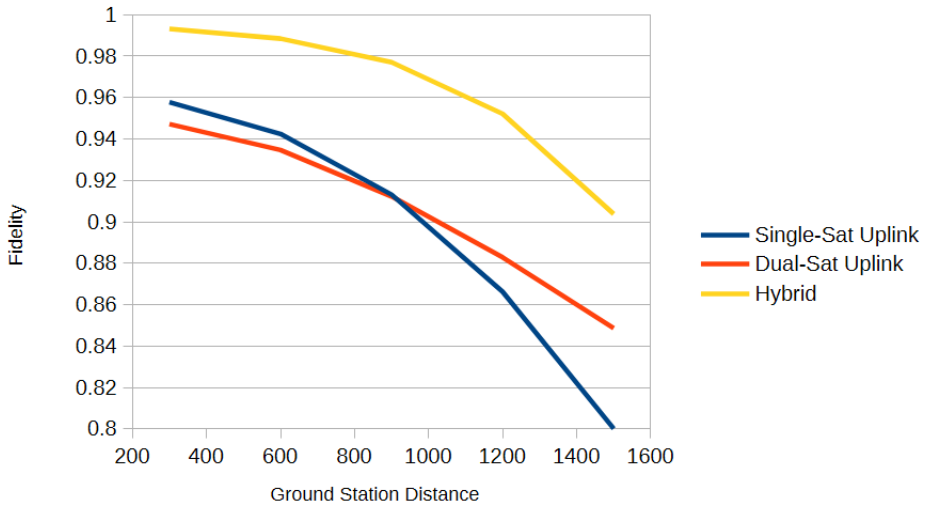

Figure 6.29: Comparison of the three architectures' fidelity as a function of ground station distance ($D_G \leq 1500$ km) for $h = 500$ km.

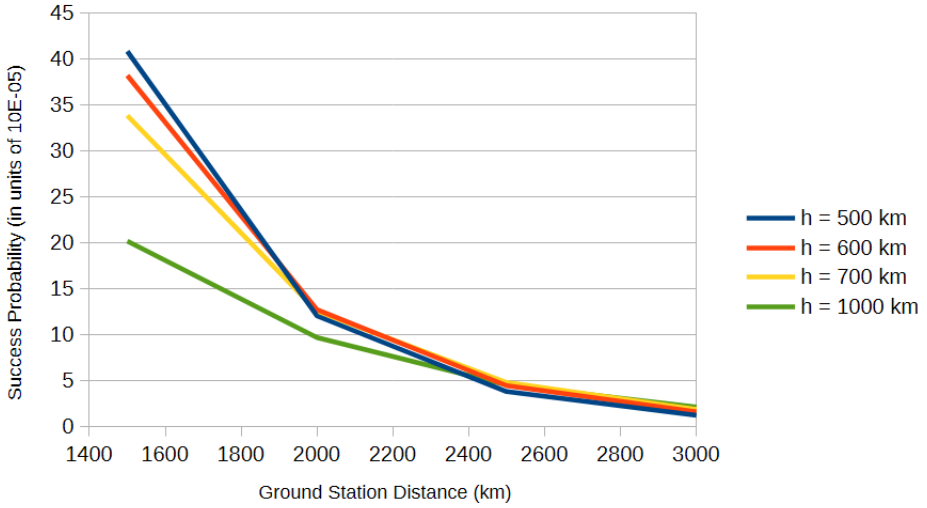

Figure 6.30: Success probability for the hybrid architecture at intercontinental scales ($D_G \geq 1500$ km) for various satellite altitudes h.

The simulation results presented in Figure 6.30 reveal a critical altitude crossover phenomenon. For ground separations below 2400 km, lower orbits (e.g., $h = 500$ km) provide superior success probabilities due to the shorter slant range. However, as the distance increases toward 3000 km, these lower orbits experience a sharp exponential decline.

This degradation is attributed to the extreme zenith angles required to maintain line-of-sight, which forces the optical signal to traverse a significantly thicker atmospheric path, leading to severe extinction. In contrast, higher orbital altitudes (e.g., $h = 1000$ km) maintain a more favorable geometry. Consequently, at the 3000 km mark, the 1000 km orbit yields a success probability that is nearly double that of the 500 km orbit, identifying higher LEO altitudes as the more robust configuration for long-range quantum backbones.

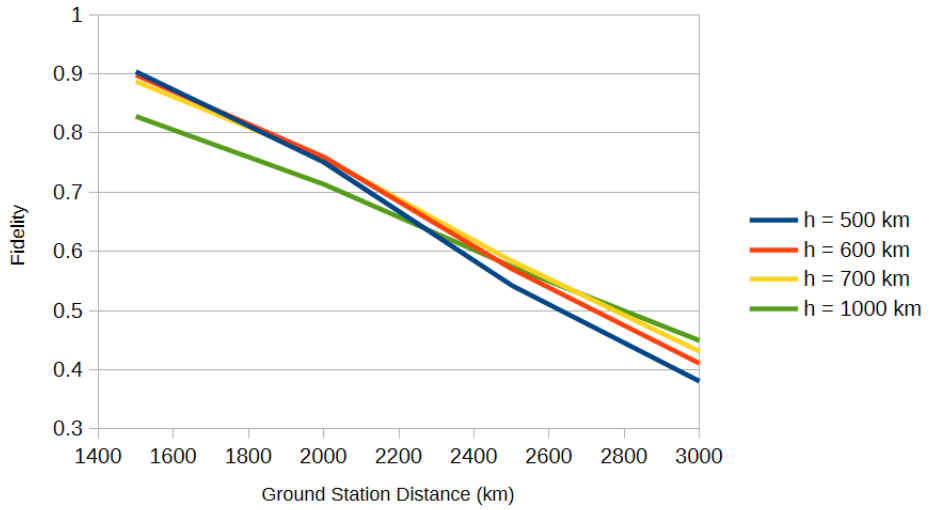

Figure 6.31: Fidelity for the hybrid architecture at intercontinental scales ($D_G \geq 1500$ km) for various satellite altitudes h.

Fidelity

As illustrated in Figure 6.31, the fidelity in the intercontinental regime is primarily governed by the Signal-to-Noise Ratio (SNR). As the ground separation grows, the total efficiency (η_{tot}) drops, causing the signal to gradually approach the noise floor ($r_n = 1500$ Hz).

Similar to the success probability, a crossover point is observed in the fidelity metrics. While lower satellites ($h = 500$ km) start with a fidelity near 0.90 at 1500 km, they degrade more rapidly, falling below 0.40 at 3000 km. High-altitude satellites ($h = 1000$ km), while starting with lower initial fidelity due to vacuum diffraction, demonstrate a more "graceful" degradation, maintaining a fidelity of $F \approx 0.45$ at the same maximum range.

The robustness of the fidelity in this architecture, even at such extreme scales, is a direct result of the absence of synchronization jitter. By replacing the stochastic losses of a second uplink with a deterministic downlink, the hybrid relay ensures that the quantum state is limited only by the link budget and background noise, rather than the temporal decoherence typically found in untrusted dual-node schemes.

6.4.4 The Trusted Node Challenge and Security Implications

A pivotal consideration in the design of global quantum networks is the security paradigm of the intermediate relay, commonly referred to as the "Trusted Node" problem. While the Hybrid Architecture demonstrates significant performance advantages in terms of success probability and fidelity, these gains are achieved by shifting the security requirements of the satellite node.

Definition of the Trusted Node Paradigm

In a trusted node configuration, the intermediate relay (the satellite) has, at some point during the protocol, access to the classical key material or the quantum state in a decodable form. This implies that the security of the entire link between Alice and Bob is no longer strictly end-to-end (E2E) based on the laws of

physics alone, but relies on the *physical and operational security* of the satellite itself. If the satellite is compromised, either through a cyber-attack on its classical processing unit or via physical tampering, the secrecy of the generated key is jeopardized.

Comparative Security Analysis

The distinction between the architectures analyzed in this study can be summarized as follows:

- **Untrusted Node (dual uplink architectures):** Utilizing Entanglement Swapping, the satellite performs a Bell State Measurement (BSM) on incoming photons. Due to the nature of quantum entanglement, the satellite remains "blind" to the final key established between Alice and Bob. This provides information-theoretic security that is independent of the relay's integrity.
- **Trusted Node (hybrid architecture):** In the hybrid relay model, the satellite essentially facilitates a point-to-point link. Security is guaranteed only if the satellite is a trusted entity. While this model is significantly more efficient, it introduces a single point of failure in the security chain.

6.5 Comparative Analysis of Satellite Quantum Architectures

In this section, we synthesize the findings from the numerical simulations to provide a comprehensive comparison of the three evaluated architectures: the Single-Satellite Dual Uplink architecture, the Dual-Satellite Dual Uplink architecture, and the Hybrid Uplink-Downlink. The comparison is based on performance scalability, hardware complexity, and security paradigms.

Note on Numerical Interpretation:

It is critical to emphasize that the numerical results presented throughout this study should not be interpreted as absolute performance metrics for any specific physical implementation. The exact values of success probability and fidelity are highly sensitive to the specific parameters of the hardware used (e.g., detector efficiency, laser power, telescope quality) and the local atmospheric conditions. Therefore, the reader should focus on the **general trends**, the **orders of magnitude**, and the **relative performance gaps** between the architectures, which remain fundamentally consistent across various physical realizations.

6.5.1 Comparative Overview

Table 6.5 summarizes the key characteristics and performance metrics of each configuration.

6.5.2 Detailed Analysis of Trade-offs

6.5.2.1 Performance and Distance Scalability

The transition from the single-satellite dual uplink architecture to the dual-satellite dual uplink architecture is driven by the need to bridge intercontinental distances. While the single-satellite architecture is

Table 6.5: Comprehensive Comparison of Quantum Satellite Architectures.

Feature	Arch 1: Single Sat	Arch 2: Dual Sat	Arch 3: Hybrid Relay
Link Type	Dual Uplink	Dual Uplink + ISL	Uplink + Downlink
Node Security	Untrusted	Untrusted	**Trusted / Semi-trusted**
Short-range ($D_G < 1500$km)	Moderate η_{tot}	Improved η_{tot}	**Maximum η_{tot} ($\sim 10^{-3}$)**
Mid-range ($1500 < D_G < 2500$km)	Geometrically Limited	Stable η_{tot}	**Superior Performance**
Extended-range ($D_G > 2500$km)	Infeasible	**Optimal / Unique Solution**	Geometrically Constrained
Fidelity Bottleneck	Jitter (x_0) + Noise	Jitter (x_0) + Loss	**Background Noise (SNR)**
Hardware Complexity	Low (1 Sat)	**Very High** (2 Sats + BSM)	Moderate (Internal Relay)
Synchronization	Crucial	Crucial	Relaxed

constrained by the geometric horizon and steep atmospheric attenuation at low elevation angles, the dual-satellite architecture utilizes the vacuum of space (ISL) to maintain connectivity up to 5000 km (optimal up to around 2200km).

However, the Hybrid Architecture emerges as the overall performance leader for short and mid-range distances. By replacing one stochastic uplink with a deterministic downlink, it exploits the Shower Curtain Effect, where the signal encounters atmospheric turbulence only at the very end of its path. This results in success probabilities that are 10 to 100 times higher than the dual-uplink models at all scales.

6.5.2.2 Hardware and Mechanical Complexity

The dual-satellite dual uplink architecture represents the pinnacle of technical difficulty. It requires two satellites to maintain a stable Inter-Satellite Link (ISL) while performing complex Bell State Measurements (BSM) in orbit. This necessitates high-precision pointing, acquisition, and tracking (PAT) systems.

In contrast, the hybrid architecture requires only an internal optical routing mechanism within a single satellite to relay the photon from the uplink receiver to the downlink transmitter. While the single-satellite dual uplink architecture is the simplest, its performance limitations at high ground separations make it less viable for global backbones.

6.5.2.3 Security Paradigm: The Trusted Node Trade-off

A fundamental divergence exists in the security models. The dual uplink architectures operate under the **untrusted node** paradigm, where the security is guaranteed by the laws of quantum mechanics even if the satellite is compromised.

The hybrid architecture, however, introduces the **Trusted Node problem**. Because the satellite acts as an active relay, it must be physically and cryptographically secured. This is a significant compromise in the “unhackable” nature of quantum communications.

6.5.3 Final Synthesis

For regional quantum networks ($D_G < 800$ km), the single-satellite dual uplink architecture remains a cost-effective choice. For "ultra-secure" intercontinental links where the satellite cannot be trusted, the dual-satellite architecture is the theoretical standard, despite its extreme complexity. The dual-satellite architecture is also the only viable solution for long range ($D_G \geq 3000km$) distances.

However, for the practical realization of a high-rate, high-fidelity global quantum internet under current technological constraints, the Hybrid Architecture provides the most robust and efficient framework, provided that sufficient trusted-node security protocols are implemented.

Chapter 7: Conclusions and Future Work

This thesis investigated the feasibility, limitations, and performance trade-offs of satellite-based quantum communication systems, with a particular emphasis on entanglement distribution architectures under realistic physical conditions. The primary objective was not only to review established protocols and technologies, but to develop a unified analytical framework capable of assessing different satellite network topologies in the presence of atmospheric loss, background noise, and spatiotemporal mode mismatch.

7.1 Summary of the Thesis

The early chapters of this thesis laid the theoretical and technological foundation necessary for the subsequent architectural analysis.

Initially, the fundamental principles of quantum information were introduced, including qubits, quantum superposition, entanglement, and measurement theory. Core quantum communication primitives such as quantum teleportation, entanglement swapping, and quantum key distribution were reviewed, establishing the conceptual basis for satellite-assisted quantum networks. Particular emphasis was placed on the physical interpretation of quantum interference and indistinguishability, as these effects play a decisive role in realistic Bell state measurements.

Subsequently, quantum communication protocols relevant to long-distance networking were examined, including prepare-and-measure and entanglement-based QKD schemes. Their security principles, operational constraints, and dependence on non-orthogonal quantum states were discussed, highlighting the importance of loss and noise modeling in practical deployments.

The thesis then transitioned to the physical layer, analyzing satellite communication link elements. Atmospheric turbulence, geometric losses, beam diffraction, background radiation, and detector noise were modeled in detail.

These chapters established the quantitative tools required to evaluate satellite quantum links beyond idealized assumptions.

7.2 Objectives and Methodology

The central goal of this thesis was to assess whether alternative satellite network architectures can mitigate the severe efficiency suppression inherent in conventional entanglement distribution schemes, particularly those relying on double-uplink entanglement swapping.

To this end, a consistent methodology was adopted throughout the work:

- A physically grounded channel model was employed, incorporating atmospheric attenuation, turbulence-induced beam spreading, background noise, and detector imperfections.
- Entanglement distribution success probability and practical fidelity were used as the primary performance metrics, enabling a joint assessment of rate and quality.
- All architectures were analyzed under comparable assumptions and parameter sets, allowing for direct and meaningful comparison.

This approach ensured that any observed performance differences arose from architectural choices rather than from inconsistent modeling assumptions.

7.3 Key Findings of the Architectural Analysis

The core contribution of this thesis is presented in Chapter 6, where three satellite-assisted entanglement distribution architectures were systematically analyzed.

7.3.1 Single-Satellite Dual-Uplink Architecture

The first architecture considered a well-established configuration in which two ground stations independently generate entangled photon pairs and transmit one photon each to a common satellite, where entanglement swapping is performed. This scheme serves as a baseline and reflects the dominant approach found in recent literature.

The analysis demonstrated that, while conceptually elegant and technologically minimal on the satellite side, this architecture suffers from a fundamental limitation: the overall success probability scales quadratically with the uplink efficiency. As a result, atmospheric turbulence, beam wandering, and limited satellite aperture sizes impose severe constraints on both achievable distance and entanglement rate. Even under favorable nighttime conditions, the operational range is restricted to regional scales, and the protocol becomes increasingly noise-dominated at larger separations.

7.3.2 Dual-Satellite Dual-Uplink Architecture

Building upon the baseline analysis, the thesis extended the framework to a dual-satellite topology, where each ground station communicates with a local satellite before an inter-satellite link enables entanglement swapping.

This architecture decouples the ground station separation from the uplink geometry, allowing both uplinks to operate near zenith and thereby significantly reducing atmospheric loss. The results demonstrated that this configuration enables intercontinental-scale entanglement distribution that is physically inaccessible to single-satellite schemes.

However, this improvement comes at the cost of increased system complexity. Precise inter-satellite pointing, sub-nanosecond temporal synchronization, and vacuum diffraction losses in the inter-satellite link introduce new engineering challenges. While the dual-satellite architecture substantially extends

operational range, its scalability is ultimately constrained by accumulated losses and synchronization requirements.

7.3.3 Hybrid Uplink–Downlink Architecture

The most significant and original contribution of this thesis is the investigation of a hybrid uplink–downlink architecture, in which entanglement is distributed without entanglement swapping. In this scheme, a single ground station generates an entangled photon pair, transmits one photon to a satellite via an uplink, and the satellite subsequently forwards the photon to a distant ground station via a downlink.

The analysis revealed a crucial scaling advantage: unlike double-uplink entanglement swapping schemes, the success probability of the hybrid architecture scales linearly with the uplink efficiency rather than quadratically. Since downlink channels are typically orders of magnitude more efficient than uplinks due to reduced turbulence and larger ground-based collection apertures, the downlink segment becomes nearly transparent compared to the uplink bottleneck.

Numerical simulations demonstrated that this architectural asymmetry leads to entanglement distribution rates several orders of magnitude higher than those achievable with double-uplink schemes at comparable distances. Importantly, this improvement is achieved without introducing additional satellites, inter-satellite synchronization, or Bell state measurements in orbit, resulting in a simpler and more robust system design.

However, this improvement comes at the cost of security as the satellite must be a trusted node.

7.4 Scientific Contribution

The contributions of this thesis can be summarized as follows:

- A unified analytical framework for evaluating satellite-based entanglement distribution architectures under realistic noise and loss conditions.
- A systematic extension of recent uplink entanglement swapping analyses to alternative network topologies.
- A quantitative demonstration that hybrid uplink-downlink architectures fundamentally outperform double-uplink schemes due to favorable efficiency scaling.
- The identification of an underexplored architectural regime that offers improved performance with reduced system complexity.

Rather than proposing a new protocol, this thesis contributes by revealing how architectural choices alone can dramatically alter the feasibility landscape of global quantum communication.

7.5 Limitations and Future Directions

While the presented results demonstrate clear advantages for hybrid architectures, several limitations remain. The analysis assumed ideal source purity, perfect polarization compensation, and classical trust in the satellite node. Future work could extend the model to include source imperfections, satellite motion-induced polarization effects, and security analyses under untrusted relay assumptions.

7.6 Final Remarks

In conclusion, this thesis shows that the feasibility of satellite-based entanglement distribution is not determined solely by technological limitations, but critically by architectural design choices. By moving beyond conventional double-uplink paradigms and systematically exploring alternative topologies, it is possible to unlock substantial performance gains using existing or near-term technology.

The results presented herein suggest that hybrid uplink–downlink architectures deserve significantly greater attention as a practical and scalable pathway toward global quantum communication networks.

7.7 Future Work and Research Directions

While this thesis demonstrates that architectural design choices alone can dramatically improve the feasibility of satellite-based entanglement distribution, several promising research directions remain open. The results presented herein naturally motivate extensions at the levels of network topology, physical layer modeling, quantum memory integration, and protocol implementation.

7.7.1 Architectural Refinements and Network-Level Extensions

A natural continuation of this work is the systematic exploration of extended network topologies derived from the proposed hybrid uplink-downlink architecture. While the present analysis focused on a single-satellite relay, multi-satellite configurations could be investigated in which hybrid links are chained to form regional or global-scale entanglement distribution networks.

In particular, constellations of Low Earth Orbit (LEO) satellites could be analyzed to determine optimal scheduling, handover strategies, and routing policies that minimize uplink bottlenecks while maximizing overall network throughput. The analytical framework developed in this thesis is readily extensible to such scenarios and could be combined with stochastic satellite motion models to evaluate time-averaged entanglement rates.

Furthermore, asymmetric architectures in which different ground stations assume distinct roles (e.g., entanglement source versus entanglement receiver) may enable more efficient resource allocation. This asymmetry could be exploited to optimize ground station placement, telescope sizing, and operational duty cycles under realistic geographical and atmospheric constraints.

7.7.2 Integration of Quantum Memories

One of the most significant limitations of near-term satellite quantum communication systems is the absence of practical quantum memories. Incorporating quantum memories at ground stations or onboard satellites represents a crucial step toward scalable quantum networks.

Future work could investigate hybrid architectures augmented with quantum memories that enable temporal multiplexing of entanglement generation attempts. Even modest memory lifetimes (on the order of milliseconds) could dramatically increase effective entanglement rates by allowing successful uplink events to be stored until a downlink transmission becomes available.

Additionally, quantum memories would enable more advanced protocols such as entanglement purification and nested entanglement swapping. The performance trade-offs between memory coherence time, storage efficiency, and system complexity constitute an open research problem, particularly in the context of space-qualified hardware.

The modeling framework presented in this thesis could be extended to include memory decoherence and storage loss, allowing for a quantitative assessment of when and where quantum memories provide a net benefit.

7.7.3 Implementation of Quantum Key Distribution Protocols

While this thesis focused primarily on entanglement distribution as a fundamental primitive, an important research direction is the explicit implementation of quantum key distribution (QKD) protocols on top of the proposed architectures.

The feasibility of daylight operation, adaptive basis selection, and dynamic filtering strategies could be investigated to assess the robustness of QKD implementations under varying environmental conditions.

A comparative study between prepare-and-measure and entanglement-based QKD protocols in hybrid satellite architectures would further clarify the operational advantages and security trade-offs of each approach.

7.7.4 Security Considerations and Trust Models

The security analysis of satellite-assisted quantum communication remains an active area of research. In this thesis, the satellite was treated as a trusted relay, which is a reasonable assumption for many near-term implementations. However, future work could relax this assumption by considering untrusted or semi-trusted satellite nodes.

Measurement-device-independent (MDI) QKD and device-independent protocols represent promising directions in this context. The extent to which hybrid uplink-downlink architectures can support such protocols, given current technological constraints, is an open question that warrants detailed investigation.

Additionally, side-channel vulnerabilities arising from timing information, spectral leakage, or polarization-dependent losses should be incorporated into future security models to bridge the gap between theoretical

and practical security guarantees.

7.7.5 Toward Global Quantum Networks

In the longer term, the architectural insights developed in this thesis contribute to the broader vision of a global quantum internet. By demonstrating that favorable scaling can be achieved without complex in-orbit operations, this work supports a design philosophy that prioritizes simplicity, robustness, and near-term deployability.

Future research could investigate how hybrid satellite architectures interface with terrestrial fiber-based quantum networks, forming heterogeneous systems that leverage the strengths of both free-space and guided media. The seamless integration of these domains remains one of the central challenges in the realization of large-scale quantum communication infrastructures.

7.8 Closing Perspective

Overall, this thesis opens multiple research paths that span theory, modeling, and experimental implementation. The proposed hybrid architectures provide a versatile platform for exploring advanced quantum communication protocols and represent a promising stepping stone toward scalable, high-performance satellite-based quantum networks.

BIBLIOGRAPHY

[1] G. E. Moore, "Cramming more components onto integrated circuits," *Electronics*, vol. 38, pp. 114–117, Apr. 1965. Reprinted in Proceedings of the IEEE, vol. 86, no. 1, pp. 82–85, Jan. 1998.

[2] H. Liu, "Quantum tunneling effect and its applications in semiconductor devices," *Highlights in Science, Engineering and Technology*, 2025.

[3] P. Kumari, "Quantum tunneling effects in ultra-scaled mosfets: A theoretical perspective on device miniaturization limits," *International Journal of Physics and Applications*, 2024.

[4] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467–488, 1982.

[5] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, pp. 117 – 97, 1985.

[6] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[7] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Symposium on the Theory of Computing*, 1996.

[8] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the darpa quantum network," *Storage and Retrieval for Image and Video Databases*, 2005.

[9] M. Peev, T. Länger, T. Lorünser, A. Happe, O. Maurhart, A. Poppe, and T. Theme, "The secoqc quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, p. 075001, 2009.

[10] M. Sasaki *et al.*, "Field test of quantum key distribution in the tokyo qkd network.," *Optics express*, vol. 19 11, pp. 10387–409, 2011.

[11] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, pp. 5932–5935, 1998.

[12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," 2001.

[13] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, pp. 1023–1030, 2008.

[14] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, 2018.

[15] P. A. M. Dirac, "A new notation for quantum mechanics," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 35, pp. 416 – 418, 1939.

[16] W. Pauli, “Zur quantenmechanik des magnetischen elektrons,” *Zeitschrift für Physik*, vol. 43, pp. 601–623, 1927.

[17] R. Shankar, *Principles of Quantum Mechanics*. New York: Plenum Press, 2 ed., 1994.

[18] I. K. Marmorkos, *Quantum Computing*. Athens: Kallipos, Hellenic Academic Libraries Link, 2024.

[19] D. P. DiVincenzo, “The physical implementation of quantum computation,” *Fortschritte der Physik*, vol. 48, p. 771–783, Sept. 2000.

[20] D. Deutsch and R. Jozsa, “Rapid solution of problems by quantum computation,” *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, vol. 439, pp. 553 – 558, 1992.

[21] D. R. Simon, “On the power of quantum computation,” in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, SFCS ’94, (USA), p. 116–123, IEEE Computer Society, 1994.

[22] R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, pp. 120–126, 1978.

[23] J. Barzen and F. Leymann, “Continued fractions and probability estimations in the shor algorithm – a detailed and self-contained treatise,” 2022.

[24] W. K. Wootters, W. K. Wootters, and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, pp. 802–803, 1982.

[25] Y.-A. Chen *et al.*, “An integrated space-to-ground quantum communication network over 4,600 kilometres,” *Nature*, vol. 589, pp. 214 – 219, 2021.

[26] S. Wang *et al.*, “Twin-field quantum key distribution over 830-km fibre,” *Nature Photonics*, vol. 16, pp. 154 – 161, 2019.

[27] N. Makris, A. Ntanos, A. Papageorgopoulos, A. Stathis, P. Konteli, I. Tsoni, G. Giannoulis, F. Setaki, T. Stathopoulos, G. Lyberopoulos, H. Avramopoulos, G. T. Kanellos, and D. Syvridis, “O-band qkd link over a multiple ont loaded carrier-grade gpon for ftth applications,” 2023.

[28] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.

[29] A. Ekert, “Quantum cryptography based on bell’s theorem.,” *Physical review letters*, vol. 67 6, pp. 661–663, 1991.

[30] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden variable theories.,” *Physical Review Letters*, vol. 23, pp. 880–884, 1969.

[31] M. S. Guimaraes, I. Roditi, and S. P. Sorella, “Introduction to bell’s inequality in quantum mechanics,” *Universe*, vol. 10, p. 396, Oct. 2024.

[32] B. S. Cirel’son, “Quantum generalizations of bell’s inequality,” *Letters in Mathematical Physics*, vol. 4, pp. 93–100, 1980.

[33] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution.," *Physical review letters*, vol. 108 13, p. 130503, 2011.

[34] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels.," *Physical review letters*, vol. 70 13, pp. 1895–1899, 1993.

[35] M. Żukowski, A. Zeilinger, M. A. Horne, and A. Ekert, ""event-ready-detectors" bell experiment via entanglement swapping.," *Physical review letters*, vol. 71 26, pp. 4287–4290, 1993.

[36] L. Duan, M. D. Lukin, I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, pp. 413–418, 2001.

[37] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics*, vol. 83, pp. 33–80, 2009.

[38] Qiskit Contributors, "Qiskit github repository." `https://github.com/Qiskit`, 2025. Accessed: 2025-12.

[39] "Ibm quantum composer." `https://quantum.cloud.ibm.com/composer`. Accessed: 2025-12.

[40] I. Dror, A. Sandrov, and N. S. Kopeika, "Experimental investigation of the influence of the relative position of the scattering layer on image quality: the shower curtain effect.," *Applied optics*, vol. 37 27, pp. 6495–9, 1998.

[41] J. Garnier and K. Sølna, "Shower curtain effect and source imaging," *Inverse Problems and Imaging*, 2024.

[42] S. P. Neumann, S. K. Joshi, M. Fink, T. Scheidl, R. Blach, C. A. Scharlemann, S. Abouagaga, D. Bambery, E. Kerstel, M. Barthélémy, and R. Ursin, "Q3sat: quantum communications uplink to a 3u cubesat—feasibility & design," *EPJ Quantum Technology*, vol. 5, 2017.

[43] S. Pirandola, "Satellite quantum communications: Fundamental bounds and practical security," *Physical Review Research*, vol. 3, 2020.

[44] D. Alaluf and J. M. P. Armengol, "Ground-to-satellite optical links: how effective is an uplink tip/tilt pre-compensation based on the satellite signal?," *CEAS Space Journal*, vol. 14, pp. 227 – 238, 2021.

[45] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New Journal of Physics*, vol. 11, p. 045017, 2009.

[46] S. Srikara, H. Leone, A. S. Solnstev, and S. J. Devitt, "Quantum entanglement distribution via uplink satellite channels," *Physical Review Research*, 2024.

[47] L. C. Andrews, W. B. Miller, and J. C. Ricklin, "Geometrical representation of gaussian beams propagating through complex paraxial optical systems.," *Applied optics*, vol. 32 30, pp. 5918–29, 1993.

[48] M. Born, E. Wolf, and E. Hecht, "Principles of optics : electromagnetic theory of propagation, interference and diffraction of light," *Physics Today*, vol. 53, pp. 77–78, 1999.

[49] R. L. Fante, "Electromagnetic beam propagation in turbulent media," *Proceedings of the IEEE*, vol. 63, pp. 1669–1692, 1975.

[50] E. long Miao, Z. Han, S. sheng Gong, Z. Tao, D. sheng Diao, and G. Guo, "Background noise of satellite-to-ground quantum key distribution," *New Journal of Physics*, vol. 7, pp. 215 – 215, 2005.

[51] P. Rohde and T. C. Ralph, "Frequency and temporal effects in linear optical quantum computing," *Physical Review A*, vol. 71, 2004.

[52] P. Rohde and T. C. Ralph, "Time-resolved detection and mode mismatch in a linear optics quantum gate," *New Journal of Physics*, vol. 13, p. 053036, 2011.

[53] K. K. Likharev, *Essential Graduate Physics — Quantum Mechanics*, vol. 2 of *Essential Graduate Physics*. Stony Brook University, 2013. Part of the lecture notes series.

[54] C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, and A. Zeilinger, "Influence of satellite motion on polarization qubits in a space-earth quantum communication link.," *Optics express*, vol. 14 21, pp. 10050–9, 2006.

[55] Q. Liu, "Doppler measurement and compensation in mobile satellite communications systems," *MILCOM 1999. IEEE Military Communications. Conference Proceedings (Cat. No.99CH36341)*, vol. 1, pp. 316–320 vol.1, 1999.

[56] H. Rouzegar and M. Ghanbarisabagh, "Estimation of doppler curve for leo satellites," *Wireless Personal Communications*, pp. 1–18, 2019.

[57] C. Simmons, P. Barrow, and R. Donaldson, "Dawn and dusk satellite quantum key distribution using time and phase based encoding and polarization filtering," *Optica Quantum*, 2024.

[58] S. Srikara, H. Leone, A. S. Solntsev, and S. J. Devitt, "Supplementary Material for "Quantum entanglement distribution via uplink satellite channels"." GitHub Repository, 2025. Accessed: 2025-01-01.

[59] R. Davidson and D. W. Miller, "Flexible design for an in-space assembled telescope," *AIAA SCITECH 2023 Forum*, 2023.

[60] F. Kunzi and O. Montenbruck, "Precise onboard time synchronization for leo satellites," *NAVIGATION: Journal of the Institute of Navigation*, 2022.

[61] A. D. C. Hernandez, E. L. Kramer, R. A. Masterson, J. J. Green, and D. W. Miller, "Rotating synthetic aperture space telescope pointing control demonstration and scalability analysis," *Journal of Spacecraft and Rockets*, 2025.

[62] M. Lake, J. E. Phelps, J. E. Dyer, D. A. Caudle, A. Tam, J. Escobedo-Torres, and E. P. Kasl, "Deployable primary mirror for space telescopes," in *Optics & Photonics*, 1999.

[63] S. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, 2017.

[64] C. Liorni, H. Kampermann, and D. Bruß, "Satellite-based links for quantum key distribution: beam effects and weather dependence," *New Journal of Physics*, vol. 21, 2019.

[65] A. V. Miller, L. V. Pismeniuk, A. V. Duplinsky, V. E. Merzlinkin, A. A. Plukchi, K. A. Tikhonova, I. S. Nesterov, D. O. Sevryukov, S. D. Levashov, V. V. Fetisov, S. V. Krasnopejev, and R. M. Bakhshaliev, "Vector—towards quantum key distribution with small satellites," *EPJ Quantum Technology*, vol. 10, pp. 1–20, 2023.

[66] J.-P. Bourgoin, E. Meyer-Scott, B. Higgins, B. Helou, C. Erven, H. Huebel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New Journal of Physics*, vol. 15, 2012.

[67] J. S. Bell and A. Aspect, *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy*. Cambridge University Press, 2 ed., 2004.

[68] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation.," *Physical review. A, Atomic, molecular, and optical physics*, vol. 52 5, pp. 3457–3467, 1995.

[69] M. Keyl, "Fundamentals of quantum information theory," *Physics Reports*, vol. 369, pp. 431–548, 2002.

[70] C. Karafyllidis, *Quantum Computing*. Athens: Kallipos, Hellenic Academic Libraries Link, 2015.

[71] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nature Physics*, vol. 5, pp. 389–392, 2009.

APPENDIX A: Entanglement swapping simulation in qiskit

```
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister
from qiskit_aer import AerSimulator

# 4 Qubits
# 0: Alice
# 1: Charlie (A)
# 2: Charlie (B)
# 3: Bob
q = QuantumRegister(4, name='q')

# BSM Charlie
cb = ClassicalRegister(2, name='cb')

# Final measurment
cf = ClassicalRegister(2, name='cf')

qc = QuantumCircuit(q, cb, cf)

# ERP AC
qc.h(q[0])
qc.cx(q[0], q[1])

# ERP BC
qc.h(q[2])
qc.cx(q[2], q[3])

qc.barrier()

#Charlies Bell measurement on q1,q2
qc.cx(q[1], q[2])
qc.h(q[1])

qc.measure(q[1], cb[0])
qc.measure(q[2], cb[1])

qc.barrier()

# Correction
# 00 (0) Φ+ -> X and Z
# 01 (1) Φ- -> X
# 10 (2) Ψ+ -> Z
# 11 (3) Ψ- -> -

with qc.if_test((cb, 0)):
    qc.x(q[0])
    qc.z(q[0])

```

```
with qc.if_test((cb, 1)):
    qc.x(q[0])

with qc.if_test((cb, 2)):
    qc.z(q[0])

qc.barrier()

#BSM q0,q3
qc.cx(q[0], q[3])
qc.h(q[0])

qc.measure(q[0], cf[0])
qc.measure(q[3], cf[1])

qc.barrier()

sim = AerSimulator()
shots = 1024
job = sim.run(qc, shots=shots)
result = job.result()
counts = result.get_counts(qc)

print("Full counts (cf cb):")
print(counts)
print()
print(qc.draw('text'))
```

Listing 3: Qiskit implementation of the Entanglement Swapping protocol.

APPENDIX B: Simulation code for the single-satellite dual uplink architecture

```

#include <iostream>
#include <cmath>
#include <functional>

////////////////////////////////////////////
// Global/Useful Constants and Helpers
////////////////////////////////////////////

static const double c_      = 299792458.0;            // Speed of light (m/s)
static const double ER      = 6.371e6;                // Earth's radius (m)
static const double pi      = 3.14159265358979323846; // Pi
static const double euler_e = 2.71828182845904523536; // e

double integrate(const std::function<double(double)>& f,
                 double a, double b,
                 int nSteps = 2000)
{
    if(a == b) return 0.0;
    double h = (b - a)/nSteps;
    double sum = 0.5*( f(a) + f(b) );
    for(int i = 1; i < nSteps; i++){
        double x = a + i*h;
        sum += f(x);
    }
    return sum * h;
}

using std::erf;

////////////////////////////////////////////////////
// 1. Wavepacket / Photonic definitions
////////////////////////////////////////////////////

double psi(double x, double x0, double sigma)
{
    double prefactor = std::pow(1.0/(2.0*pi*sigma*sigma), 0.25);
    double exponent  = -0.25*std::pow((x - x0)/sigma, 2);
    return prefactor * std::exp(exponent);
}

double psi1(double x, double x0, double sigma)
{
    return psi(x, 0.0, sigma);
}

double psi2(double x, double x0, double sigma)
```

```
{
    return psi(x, x0, sigma);
}

double Pgw1(double x0, double sigma, double tmin, double tmax)
{
    double a = c_*tmin;
    double b = c_*tmax;
    auto integrand = [x0, sigma](double x){
        double val = psi1(x, x0, sigma);
        return val*val;
    };
    return integrate(integrand, a, b);
}

double Pgw2(double x0, double sigma, double tmin, double tmax)
{
    double a = c_*tmin;
    double b = c_*tmax;
    auto integrand = [x0, sigma](double x){
        double val = psi2(x, x0, sigma);
        return val*val;
    };
    return integrate(integrand, a, b);
}

double GammaVal(double x0, double sigma, double tmin, double tmax)
{
    double a = c_*tmin;
    double b = c_*tmax;
    auto integrand = [x0, sigma](double x){
        return psi1(x, x0, sigma)*psi2(x, x0, sigma);
    };
    double val = integrate(integrand, a, b);
    return val*val;
}

double Fic(double x0, double sigma, double tmin, double tmax)
{
    double pgw1 = Pgw1(x0, sigma, tmin, tmax);
    double pgw2 = Pgw2(x0, sigma, tmin, tmax);
    double gamma = GammaVal(x0, sigma, tmin, tmax);
    if(pgw1 <= 0.0 || pgw2 <= 0.0) return 0.5;
    return 0.5 + gamma/(2.0*pgw1*pgw2);
}

////////////////////////////////////////////////////
// 2. Geometries, angles, distances, etc.
////////////////////////////////////////////////////

double zTheta(double h, double theta)
{
    return std::sqrt(h*h + 2.0*h*ER + ER*ER*std::cos(theta)*std::cos(theta))
```

```
            - ER*std::cos(theta);
}

double zAlpha(double h, double alpha)
{
    double R  = ER + h;
    double cA = std::cos(alpha);
    return std::sqrt(ER*ER + R*R - 2.0*ER*R*cA);
}

double AlphaAngle(double h, double theta)
{
    double numer = ER + zTheta(h, theta)*std::cos(theta);
    double denom = ER + h;
    double ratio = numer/denom;
    if(ratio > 1.0) ratio = 1.0;
    if(ratio < -1.0) ratio = -1.0;
    return std::acos(ratio);
}

double hTheta(double z, double theta)
{
    return std::sqrt(ER*ER + z*z + 2.0*z*ER*std::cos(theta)) - ER;
}

double alpha2(double h, double theta1, double DG)
{
    return (DG/ER) - AlphaAngle(h, theta1);
}

double theta2(double h, double theta1, double DG)
{
    double a2 = alpha2(h, theta1, DG);
    double R  = ER + h;
    double cA2 = std::cos(a2);
    double zA2 = zAlpha(h, a2);
    double ratio = (R*cA2 - ER)/zA2;
    if(ratio>1.0) ratio=1.0;
    if(ratio<-1.0) ratio=-1.0;
    return std::acos(ratio);
}

double theta_e(double h, double DG)
{
    double halfDGoverER = (DG/(2.0*ER));
    double R  = ER + h;
    double cVal = std::cos(halfDGoverER);
    double top = (R*cVal - ER);
    double zA  = zAlpha(h, halfDGoverER);
    double ratio = top / zA;
    if(ratio>1.0) ratio=1.0;
    if(ratio<-1.0) ratio=-1.0;
    return std::acos(ratio);
```

```
}

////////////////////////////////////////////////////
// 3. Beam Widening and Transmission
////////////////////////////////////////////////////

static const double Cw = 2.2354e-12;

double Kappa0(double theta, double lambda)
{
    double val = 1.46 * std::pow((2.0*pi/lambda),2.0) * (1.0/std::cos(theta)) * Cw;
    return std::pow(val, -3.0/5.0);
}

double wSquared(double w0, double z, double lambda, double K0)
{
    double term1 = w0*w0 * (1.0 + std::pow( (z*lambda)/(pi*w0*w0), 2.0));
    double term2 = 2.0 * std::pow( (lambda*z)/(pi*K0), 2.0 );
    return term1 + term2;
}

double eta_w(double RA, double wSq, double z, double sigma_tr)
{
    double denom = wSq + (z*1e-6)*(z*1e-6) + sigma_tr*sigma_tr;
    double arg   = -2.0*(RA*RA)/denom;
    return 1.0 - std::exp(arg);
}

////////////////////////////////////////////////////
// 4. Atmospheric Efficiency
////////////////////////////////////////////////////

static const double alpha0 = 5e-6;
static const double hTilde = 6600.0;

double eta_a(double h, double theta)
{
    double zt = zTheta(h, theta);
    if(zt <= 0.0) return 1.0;
    auto integrand = [theta](double y){
        double val = hTheta(y, theta)/hTilde;
        return std::exp(-val);
    };
    double val = integrate(integrand, 0.0, zt);
    double exponent = -alpha0*val;
    return std::exp(exponent);
}

////////////////////////////////////////////////////
// 5. Overall Single-Photon Channel Efficiency
////////////////////////////////////////////////////

double eta_ph(double RA, double w0, double h, double theta,
```

```
207                 double lambda, double sigma_tr, double eta_m)
208 {
209     double K0 = Kappa0(theta, lambda);
210     double z  = zTheta(h, theta);
211     double wsq = wSquared(w0, z, lambda, K0);
212     double eW  = eta_w(RA, wsq, z, sigma_tr);
213     double eA  = eta_a(h, theta);
214     return eW * eA * eta_m;
215 }
216
217 double etaA(double RA, double w0, double h, double theta,
218             double lambda, double sigma_tr, double eta_m,
219             double x0, double sigma, double tmin, double tmax)
220 {
221     return eta_ph(RA, w0, h, theta, lambda, sigma_tr, eta_m)
222          * Pgw1(x0, sigma, tmin, tmax);
223 }
224 double etaB(double RA, double w0, double h, double theta,
225             double lambda, double sigma_tr, double eta_m,
226             double x0, double sigma, double tmin, double tmax)
227 {
228     return eta_ph(RA, w0, h, theta, lambda, sigma_tr, eta_m)
229          * Pgw2(x0, sigma, tmin, tmax);
230 }
231
232 ////////////////////////////////////////////////////
233 // 6. Stray Photons (Night)
234 ////////////////////////////////////////////////////
235
236 static const double EE = 0.3;         // Earth's Albedo
237 static const double IS = 4.61e27;     // Solar spectral irradiance (SI)
238 static const double M  = 0.14;        // Moon albedo
239 static const double rM = 1737.4e3;    // Moon radius (m)
240 static const double lME= 363300e3;    // Earth-moon dist. (m)
241 static const double p_ = 6.626e-34;   // Planck's const
242 static const double kB = 1.381e-23;   // Boltzmann's const
243
244 double ND(double RA, double thetaFOV)
245 {
246     return EE * IS * std::pow(RA*thetaFOV, 2.0);
247 }
248
249 double IBB(double lambda, double T)
250 {
251     double top = 2.0*c_/(std::pow(lambda, 4.0));
252     double expo= p_*c_/(lambda*kB*T);
253     double denom= std::exp(expo) - 1.0;
254     return top*(1.0/denom);
255 }
256
257 double NN(double lambda, double T, double RA, double thetaFOV)
258 {
259     double firstTerm = pi*IBB(lambda, T)*std::pow(RA*thetaFOV,2.0);
```

```
    double secondTerm= ND(RA,thetaFOV)* M * std::pow(rM/lME,2.0);
    return firstTerm + secondTerm;
}

double rnight(double CD, double h, double theta, double eta_m,
              double RA, double thetaFOV, double DeltaLambda,
              double lambda, double T)
{
    double val = 0.5*eta_a(h,theta)*eta_m*NN(lambda, T, RA, thetaFOV)*DeltaLambda;
    return CD + val;
}

static double factorial(int n) {
    double f = 1.0;
    for(int i=1; i<=n; i++) f *= (double)i;
    return f;
}
double Psp(int n, double r, double t)
{
    double rt = r*t;
    double top = std::pow(rt, (double)n)*std::exp(-rt);
    double bot = factorial(n);
    return top/bot;
}

////////////////////////////////////////////////////
// 7. Probability of Detector "Click" Patterns
////////////////////////////////////////////////////

double Pm1010(double PG0, double PG1, double PG2,
              double PD0, double PD1, double PD2)
{
    return PG2*(PD0 + 2.0*PD1 + PD2) + 2.0*PG1*(PD1+PD2) + PG0*PD2;
}

double EtaTot(double PG0, double PG1, double PG2,
              double PD0, double PD1, double PD2)
{
    return 4.0 * Pm1010(PG0, PG1, PG2, PD0, PD1, PD2);
}

double PS(double PG0, double PG1, double PG2,
          double PD0, double PD1, double PD2)
{
    double numerator   = PG2*(PD0 + 2.0*PD1 + PD2);
    double denominator = Pm1010(PG0, PG1, PG2, PD0, PD1, PD2);
    if(denominator <= 0.0) return 0.0;
    return numerator/denominator;
}

double Fval(double PG0, double PG1, double PG2,
            double PD0, double PD1, double PD2,
            double x0, double sigma, double tmin, double tmax)
```

```
{
    double psval = PS(PG0, PG1, PG2, PD0, PD1, PD2);
    double fic   = Fic(x0, sigma, tmin, tmax);
    return psval*fic + (1.0 - psval)*(0.25);
}

////////////////////////////////////////////////////
// 8. Auxiliary: PG0, PG1, PG2 and PD0, PD1, PD2
////////////////////////////////////////////////////

double PG0(double etaA, double etaB)
{
    return (1.0 - etaA)*(1.0 - etaB);
}

double PG1(double etaA, double etaB)
{
    double firstTerm = (etaA*(1.0-etaB) + etaB*(1.0-etaA))*0.25;
    double secondTerm= 0.0625*etaA*etaB;
    return firstTerm + secondTerm;
}

double PG2(double etaA, double etaB)
{
    return 0.125*etaA*etaB;
}

double PD0(double psp0)
{
    return std::pow(psp0, 4.0);
}

double PD1(double psp0)
{
    return std::pow(psp0,3.0)*(1.0 - psp0);
}

double PD2(double psp0)
{
    double t1 = std::pow(psp0,2.0);
    double t2 = std::pow(1.0-psp0,2.0);
    return t1*t2;
}

////////////////////////////////////////////////////
// 9. Final Nighttime Functions
////////////////////////////////////////////////////

double EtaTotNight(double RA, double w0, double h,
                   double theta, double theta2_,
                   double lambda, double sigma_tr, double eta_m,
                   double x0, double sigma, double tmin, double tmax,
                   double CD, double thetaFOV, double DeltaLambda,
```

```
                    double T)
{
    double eA = etaA(RA, w0, h, theta,  lambda, sigma_tr, eta_m, x0, sigma, tmin,
    tmax);
    double eB = etaB(RA, w0, h, theta2_,lambda, sigma_tr, eta_m, x0, sigma, tmin,
    tmax);
    double pg0 = PG0(eA, eB);
    double pg1 = PG1(eA, eB);
    double pg2 = PG2(eA, eB);

    double rn  = rnight(CD, h, theta, eta_m, RA, thetaFOV, DeltaLambda, lambda, T);
    double dt  = (tmax - tmin);

    double p0  = Psp(0, rn, dt);
    double pd0 = PD0(p0);
    double pd1 = PD1(p0);
    double pd2 = PD2(p0);

    return EtaTot(pg0, pg1, pg2, pd0, pd1, pd2);
}

double Fnight(double RA, double w0, double h,
              double theta, double theta2_,
              double lambda, double sigma_tr, double eta_m,
              double x0, double sigma, double tmin, double tmax,
              double CD, double thetaFOV, double DeltaLambda,
              double T)
{
    double eA = etaA(RA, w0, h, theta,  lambda, sigma_tr, eta_m, x0, sigma, tmin,
    tmax);
    double eB = etaB(RA, w0, h, theta2_,lambda, sigma_tr, eta_m, x0, sigma, tmin,
    tmax);
    double pg0 = PG0(eA, eB);
    double pg1 = PG1(eA, eB);
    double pg2 = PG2(eA, eB);

    double rn  = rnight(CD, h, theta, eta_m, RA, thetaFOV, DeltaLambda, lambda, T);
    double dt  = (tmax - tmin);

    double p0  = Psp(0, rn, dt);
    double pd0 = PD0(p0);
    double pd1 = PD1(p0);
    double pd2 = PD2(p0);

    return Fval(pg0, pg1, pg2, pd0, pd1, pd2, x0, sigma, tmin, tmax);
}


int main()
{
    // Example parameters:
    double CD    = 1500.0;
    double hVal  = 600e3;      // satellite altitude
```

```
    double DG    = 1000e3;     // gorund separation
    double RA    = 0.75;
    double w0    = 0.13;
    double thetaFOV = 1.0e-5;
    double DeltaLambda = 1.0e-9;
    double lambda_     = 8.0e-7;    // 800 nm
    double T_          = 300.0;     // K
    double cSpeed      = 3.0e8;
    double eta_m       = 0.25;
    double sigma_t     = 10e-9*cSpeed;  // wavepacket width in meters
    double tmin_       = -(40e-9)/2 + 10e-9;   // gating window
    double tmax_       =  (40e-9)/2 + 10e-9;
    double x0_         = cSpeed*(3e-9);  // path difference
    double sigma_tr    = 0.1;        // tracking error (m)

    // The "equidistant" angles:
    double th1 = theta_e(hVal, DG);
    double th2 = th1; // symmetrical

    // Evaluate night-time success probability and fidelity:
    double etaNight = EtaTotNight(RA, w0, hVal, th1, th2,
                                  lambda_, sigma_tr, eta_m,
                                  x0_, sigma_t, tmin_, tmax_,
                                  CD, thetaFOV, DeltaLambda,
                                  T_);
    double fNight   = Fnight(RA, w0, hVal, th1, th2,
                             lambda_, sigma_tr, eta_m,
                             x0_, sigma_t, tmin_, tmax_,
                             CD, thetaFOV, DeltaLambda,
                             T_);

    std::cout << "Nighttime Success Probability = " << etaNight << "\n";
    std::cout << "Nighttime Fidelity            = " << fNight   << "\n";

    return 0;
}
```

Listing 4: C++ implementation of the single-satellite dual uplink architecture.

APPENDIX C: Simulation code for the dual-satellite dual uplink architecture

```cpp
#include <iostream>
#include <cmath>
#include <functional>
#include <vector>

////////////////////////////////////////////
// Global/Useful Constants
////////////////////////////////////////////

static const double c_      = 299792458.0;            // Speed of light (m/s)
static const double ER      = 6371000.0;              // Earth's radius (m)
static const double pi      = 3.14159265358979323846; // Pi
static const double euler_e = 2.71828182845904523536; // e

// Integration Helper (Trapezoidal)
double integrate(const std::function<double(double)>& f, double a, double b, int
    nSteps = 2000)
{
    if(std::abs(a - b) < 1e-9) return 0.0;
    double h = (b - a)/nSteps;
    double sum = 0.5*( f(a) + f(b) );
    for(int i = 1; i < nSteps; i++){
        double x = a + i*h;
        sum += f(x);
    }
    return sum * h;
}

////////////////////////////////////////////////////
// 1. Wavepacket / Photonic definitions
////////////////////////////////////////////////////

double psi(double x, double x0, double sigma)
{
    // Gaussian Wavepacket: (1/(2*pi*sigma^2))^(1/4) * exp(...)
    double prefactor = std::pow(1.0/(2.0*pi*sigma*sigma), 0.25);
    double exponent  = -0.25*std::pow((x - x0)/sigma, 2);
    return prefactor * std::exp(exponent);
}

double Pgw1(double x0, double sigma, double tmin, double tmax)
{
    double a = c_*tmin;
    double b = c_*tmax;
    auto integrand = [x0, sigma](double x){
        double val = psi(x, 0.0, sigma); // Centered at 0
        return val*val;
```

```
    };
    return integrate(integrand, a, b);
}

double Pgw2(double x0, double sigma, double tmin, double tmax)
{
    double a = c_*tmin;
    double b = c_*tmax;
    auto integrand = [x0, sigma](double x){
        double val = psi(x, x0, sigma); // Centered at x0 (mismatch)
        return val*val;
    };
    return integrate(integrand, a, b);
}

// Overlap integral gamma
double GammaVal(double x0, double sigma, double tmin, double tmax)
{
    double a = c_*tmin;
    double b = c_*tmax;
    auto integrand = [x0, sigma](double x){
        return psi(x, 0.0, sigma) * psi(x, x0, sigma);
    };
    double val = integrate(integrand, a, b);
    return val*val; // absolute square
}

// Interference Fidelity (F_ic) due to mode mismatch
double Fic(double x0, double sigma, double tmin, double tmax)
{
    double pgw1 = Pgw1(x0, sigma, tmin, tmax);
    double pgw2 = Pgw2(x0, sigma, tmin, tmax);
    double gamma = GammaVal(x0, sigma, tmin, tmax);

    if(pgw1 <= 1e-20 || pgw2 <= 1e-20) return 0.5;
    return 0.5 + gamma/(2.0*pgw1*pgw2);
}

////////////////////////////////////////////////////
// 2. Beam Widening & Channel Physics
////////////////////////////////////////////////////

// Turbulence parameters
static const double Cw = 2.2354e-12; // Refractive index structure constant profile

double Kappa0(double theta, double lambda)
{
    // Coherence length (Atmosphere)
    double secTheta = 1.0/std::cos(theta);
    double k = 2.0*pi/lambda;
    double val = 1.46 * k*k * secTheta * Cw;
    return std::pow(val, -3.0/5.0);
}
```

```
100
101 // Beam width squared for Uplink (Turbulence + Diffraction)
102 double wSquared_Uplink(double w0, double z, double lambda, double K0)
103 {
104     double term1 = w0*w0 * (1.0 + std::pow( (z*lambda)/(pi*w0*w0), 2.0));
105     double term2 = 2.0 * std::pow( (lambda*z)/(pi*K0), 2.0 );
106     return term1 + term2;
107 }
108
109 // NEW: Beam width squared for ISL (Diffraction Only - Vacuum)
110 double wSquared_ISL(double w0, double L, double lambda)
111 {
112     double term = (L * lambda) / (pi * w0 * w0);
113     return w0 * w0 * (1.0 + term * term);
114 }
115
116 // Collection Efficiency (Geometric)
117 double eta_geometric(double RA, double wSq, double z_or_L, double sigma_tr)
118 {
119     double denom = wSq + std::pow(z_or_L * 1e-6, 2.0) + sigma_tr*sigma_tr;
120     // Note: z*1e-6 is a small correction usually ignored or used for pointing
    jitter scaling.
121     // For pure pointing error sigma_tr is the main term.
122     double arg   = -2.0*(RA*RA)/(wSq + sigma_tr*sigma_tr); // Simplified standard
    form
123     return 1.0 - std::exp(arg);
124 }
125
126 ////////////////////////////////////////////////
127 // 3. Atmospheric Extinction
128 ////////////////////////////////////////////////
129
130 static const double alpha0 = 5e-6;  // Extinction coeff at sea level
131 static const double hTilde = 6600.0; // Scale height
132
133 double zTheta(double h, double theta) {
134     return std::sqrt(h*h + 2.0*h*ER + ER*ER*std::cos(theta)*std::cos(theta)) - ER*
    std::cos(theta);
135 }
136
137 double hTheta(double z, double theta) {
138     return std::sqrt(ER*ER + z*z + 2.0*z*ER*std::cos(theta)) - ER;
139 }
140
141 double eta_atm(double h, double theta)
142 {
143     double zt = zTheta(h, theta);
144     auto integrand = [theta](double y){
145         double val = hTheta(y, theta)/hTilde;
146         return std::exp(-val);
147     };
148     double val = integrate(integrand, 0.0, zt, 500);
149     return std::exp(-alpha0 * val);
```

```
}

////////////////////////////////////////////////////
// 4. Noise Models (Night)
////////////////////////////////////////////////////

static const double EE = 0.3;         // Earth Albedo
static const double IS = 4.61e27;     // Solar spectral irradiance
static const double M  = 0.14;        // Moon albedo
static const double rM = 1737.4e3;    // Moon radius
static const double lME= 363300e3;    // Earth-moon dist
static const double p_ = 6.626e-34;   // Planck
static const double kB = 1.381e-23;   // Boltzmann

double ND(double RA, double thetaFOV) { return EE * IS * std::pow(RA*thetaFOV, 2.0);
     }

double IBB(double lambda, double T) {
    double top = 2.0*c_/(std::pow(lambda, 4.0));
    double expo= p_*c_/(lambda*kB*T);
    return top/(std::exp(expo) - 1.0);
}

double NN(double lambda, double T, double RA, double thetaFOV) {
    // Thermal + Moonlight
    double term1 = pi*IBB(lambda, T)*std::pow(RA*thetaFOV,2.0);
    double term2 = ND(RA,thetaFOV)* M * std::pow(rM/lME,2.0);
    return term1 + term2;
}

double rnight(double CD, double h, double theta, double eta_m,
              double RA, double thetaFOV, double DeltaLambda,
              double lambda, double T)
{
    double etaA = eta_atm(h, theta);
    // Stray photons collected * atmospheric transmission * measurement efficiency
    double stray = 0.5 * etaA * eta_m * NN(lambda, T, RA, thetaFOV) * DeltaLambda;
    return CD + stray;
}

// Poisson Probability
double Psp(int n, double r, double t)
{
    double rt = r*t;
    if(n==0) return std::exp(-rt);
    return std::pow(rt, (double)n) * std::exp(-rt) / (double)1.0; // Simplified for
    n=0,1...
}

////////////////////////////////////////////////////
// 5. Probability Logic (Signal & Noise)
////////////////////////////////////////////////////

```

```
// Helper for Signal Probabilities
double PG0(double etaA, double etaB) { return (1.0 - etaA)*(1.0 - etaB); }
double PG1(double etaA, double etaB) { return 0.25*(etaA*(1.0-etaB) + etaB*(1.0-etaA)) + 0.0625*etaA*etaB; }
double PG2(double etaA, double etaB) { return 0.125*etaA*etaB; }

// Helper for Noise Probabilities (from Poisson p0)
double PD0(double p0) { return std::pow(p0, 4.0); }
double PD1(double p0) { return std::pow(p0, 3.0)*(1.0 - p0); }
double PD2(double p0) { return std::pow(p0, 2.0)*std::pow(1.0-p0, 2.0); }

// Probability of pattern 1010 (One click L, One click R)
double Pm1010(double PG0, double PG1, double PG2, double PD0, double PD1, double PD2)
{
    return PG2*(PD0 + 2.0*PD1 + PD2) + 2.0*PG1*(PD1+PD2) + PG0*PD2;
}

double EtaTot(double PG0, double PG1, double PG2, double PD0, double PD1, double PD2)
{
    return 4.0 * Pm1010(PG0, PG1, PG2, PD0, PD1, PD2);
}

double PS(double PG0, double PG1, double PG2, double PD0, double PD1, double PD2)
{
    double num = PG2*(PD0 + 2.0*PD1 + PD2);
    double den = Pm1010(PG0, PG1, PG2, PD0, PD1, PD2);
    return (den > 0.0) ? num/den : 0.0;
}

////////////////////////////////////////////////////
// 6. DUAL SATELLITE CORE FUNCTION
////////////////////////////////////////////////////

void SimulateDualSat(double DG_Ground, double h, double RA, double w0,
                     double lambda, double sigma_tr, double eta_m,
                     double x0, double sigma_t, double t_gate,
                     double CD, double thetaFOV, double DeltaLambda, double T)
{
    // A. Geometry
    double theta_vertical = 0.3; // Vertical Uplink
    double L_ISL = DG_Ground * (ER + h) / ER; // Arc length at altitude h

    // B. Efficiencies
    // 1. Uplink Efficiency (Common for Alice & Bob)
    double K0 = Kappa0(theta_vertical, lambda);
    double z_up = h; // Vertical distance
    double wSq_up = wSquared_Uplink(w0, z_up, lambda, K0);
    double e_geo_up = eta_geometric(RA, wSq_up, z_up, sigma_tr);
    double e_atm_up = eta_atm(h, theta_vertical);

    // Total pure photon efficiency for one vertical uplink
```

```
    double eta_Uplink_Pure = e_geo_up * e_atm_up * eta_m;

    // 2. ISL Efficiency (Vacuum)
    double wSq_isl = wSquared_ISL(w0, L_ISL, lambda);
    double e_isl = eta_geometric(RA, wSq_isl, L_ISL, sigma_tr);

    // 3. Combined Link Efficiencies
    // Alice must survive Uplink AND ISL
    double etaA_total = eta_Uplink_Pure * e_isl * Pgw1(x0, sigma_t, -t_gate/2,
    t_gate/2);
    // Bob must survive only Uplink
    double etaB_total = eta_Uplink_Pure * Pgw2(x0, sigma_t, -t_gate/2, t_gate/2);

    // C. Noise Calculation
    // Base Uplink Noise rate (Vertical)
    double r_noise_base = rnight(CD, h, theta_vertical, eta_m, RA, thetaFOV,
    DeltaLambda, lambda, T);

    // Noise arriving at Sat2 (Where BSM happens)
    // From Bob: Direct Uplink noise
    double r_noise_Bob = r_noise_base;
    // From Alice: Uplink noise attenuated by ISL
    double r_noise_Alice = r_noise_base * e_isl;

    // Conservative Estimate: Use the higher noise (Bob's) for the Poisson
    statistics
    // This gives a lower bound on Fidelity (Safe scientific assumption)
    double r_effective = r_noise_Bob;

    // D. Probabilities
    double pg0 = PG0(etaA_total, etaB_total);
    double pg1 = PG1(etaA_total, etaB_total);
    double pg2 = PG2(etaA_total, etaB_total);

    double p0_noise = Psp(0, r_effective, t_gate);
    double pd0 = PD0(p0_noise);
    double pd1 = PD1(p0_noise);
    double pd2 = PD2(p0_noise);

    // E. Final Metrics
    double SuccessProb = EtaTot(pg0, pg1, pg2, pd0, pd1, pd2);

    double P_Signal = PS(pg0, pg1, pg2, pd0, pd1, pd2);
    double F_interference = Fic(x0, sigma_t, -t_gate/2, t_gate/2);
    double Fidelity = P_Signal * F_interference + (1.0 - P_Signal) * 0.25;

    std::cout << DG_Ground/1000.0 << "\t"
              << SuccessProb << "\t"
              << Fidelity << "\t"
              << e_isl << "\n"; // Also printing ISL efficiency to check losses
}

int main()
```

```
{
    // PARAMETERS
    double h         = 600e3;      // 500 km Altitude
    double RA        = 0.75;       // 75 cm Radius (1.5m Diameter)
    double w0        = 0.13;      // Initial beam waist
    double lambda    = 800e-9;     // 800 nm
    double sigma_tr  = 0.1;        // Tracking error (m)
    double eta_m     = 0.25;       // Measurement efficiency

    // Timing
    double sigma_t   = 10e-9 * c_; // 10 ns (spatial)
    double t_gate    = 40e-9;      // 40 ns window
    double x0        = 5e-9 * c_;  // 5 ns jitter (spatial)

    // Noise
    double CD           = 1500.0;
    double thetaFOV     = 1.0e-5;
    double DeltaLambda  = 1.0e-9;
    double T            = 300.0;

    std::cout << "--- Dual Satellite Simulation (Arch 2) ---\n";
    std::cout << "Dist(km)\tSuccessProb\tFidelity\tISL_Eff\n";

    // Sweep Ground Distance from 1000 km to 20,000 km
    for(double dist = 1500e3; dist <= 5000e3; dist += 500e3)
    {
        SimulateDualSat(dist, h, RA, w0, lambda, sigma_tr, eta_m,
                        x0, sigma_t, t_gate, CD, thetaFOV, DeltaLambda, T);
    }


    return 0;
}
```

Listing 5: C++ implementation of the dual-satellite dual uplink architecture.

APPENDIX D: Simulation code for the hybrid uplink-downlink architecture

```cpp
#include <iostream>
#include <cmath>
#include <functional>
#include <iomanip>

/**
 * ARCHITECTURE 3: HYBRID QUANTUM RELAY
 * Model: Ground (Alice) -> Satellite (Relay) -> Ground (Bob)
 * This code simulates the link budget, success probability, and fidelity
 * for a single-photon relay architecture under nighttime conditions.
 */

// Global Constants
static const double c_      = 299792458.0;            // Speed of light (m/s)
static const double ER      = 6371000.0;              // Earth's radius (m)
static const double pi      = 3.14159265358979323846;

// --- GEOMETRY MODULE ---
struct Geometry {
    double z;     // Slant range (m)
    double theta; // Zenith angle (rad)
};

// Calculates the slant range and zenith angle based on ground distance DG and altitude h
Geometry calculateGeometry(double h, double DG) {
    double alpha = (DG / (2.0 * ER)); // Central angle for half the ground distance
    double R = ER + h;

    // Law of Cosines to find slant range (z)
    double z = std::sqrt(ER*ER + R*R - 2.0*ER*R*std::cos(alpha));

    // Calculate Zenith Angle (theta)
    double ratio = (R * std::cos(alpha) - ER) / z;
    if(ratio > 1.0) ratio = 1.0;
    if(ratio < -1.0) ratio = -1.0;

    return {z, std::acos(ratio)};
}

// Auxiliary function to find height at any point along the path for atmospheric integration
double h_at_dist(double y, double theta) {
    return std::sqrt(ER*ER + y*y + 2.0*y*ER*std::cos(theta)) - ER;
}

// --- ATMOSPHERIC EXTINCTION MODULE ---
```

```
// Trapezoidal rule for integration
double integrate(const std::function<double(double)>& f, double a, double b, int nSteps = 1000) {
    if(a >= b) return 0.0;
    double h = (b - a)/nSteps;
    double sum = 0.5*( f(a) + f(b) );
    for(int i = 1; i < nSteps; i++) sum += f(a + i*h);
    return sum * h;
}

// Beer-Lambert Exponential Extinction
double eta_atmospheric(double z, double theta) {
    static const double alpha0 = 5e-6;   // Nighttime extinction coefficient
    static const double hTilde = 6600.0; // Scale height (m)
    auto integrand = [theta](double y){ return std::exp(-h_at_dist(y, theta)/hTilde); };
    return std::exp(-alpha0 * integrate(integrand, 0.0, z));
}

// --- BEAM PROPAGATION MODULE ---

// Uplink: Includes both Diffraction and Atmospheric Turbulence spreading
double wSquaredUplink(double w0, double z, double lambda, double theta) {
    static const double Cw = 2.2354e-12; // Standard nighttime turbulence constant

    // Coherence length K0 (Kolmogorov model)
    double K0 = std::pow(1.46 * std::pow(2.0*pi/lambda, 2.0) * (1.0/std::cos(theta)) * Cw, -3.0/5.0);

    double w_diff_sq = w0*w0 * (1.0 + std::pow((z*lambda)/(pi*w0*w0), 2.0)); // Diffraction term
    double w_turb_sq = 2.0 * std::pow((lambda*z)/(pi*K0), 2.0);             // Turbulence term

    return w_diff_sq + w_turb_sq;
}

// Downlink: Diffraction-limited only (Shower Curtain Effect)
double wSquaredDownlink(double w0, double z, double lambda) {
    return w0*w0 * (1.0 + std::pow((z*lambda)/(pi*w0*w0), 2.0));
}

// Geometric Collection Efficiency at the aperture
double collection_efficiency(double R_rec, double wSq, double sigma_tr) {
    // sigma_tr represents the Pointing Jitter (RMS displacement)
    return 1.0 - std::exp(-2.0*R_rec*R_rec / (wSq + sigma_tr*sigma_tr));
}

// --- CORE SIMULATION ---
void runSimulation(double h, double DG) {
    // --- System Parameters ---
    double lambda = 800e-9;      // Wavelength (800nm)
    double w0 = 0.13;            // Initial beam waist (m)
```

```
    double sigma_tr = 0.1;        // Pointing jitter (m)
    double Rsat = 0.75;          // Satellite receiver aperture
    double Rground = 0.75;        // Bob ground receiver
    double eta_relay = 0.90;      // Internal Satellite relay efficiency (mirrors/
    optics)
    double det_eff = 0.25;        // Bob's ground detector efficiency

    // --- Noise & Timing Parameters  ---
    double rn = 1500.0;           // Night background noise + Dark counts (Hz)
    double dt = 40e-9;            // Gating window t_gate = 40ns
    // sigma_t = 10ns is assumed to be contained within dt

    // 1. Geometry Calculation
    Geometry geo = calculateGeometry(h, DG);

    // Check if the satellite is below the horizon (Horizon limit approx theta ~ 1.5
     rad)
    if(geo.theta > 1.55) {
        std::cout << std::setw(10) << DG/1000.0 << " | Out of Sight" << std::endl;
        return;
    }

    // 2. Uplink Segment (Alice at Ground -> Satellite Relay)
    double wSqA = wSquaredUplink(w0, geo.z, lambda, geo.theta);
    double eta_up = collection_efficiency(Rsat, wSqA, sigma_tr) * eta_atmospheric(
    geo.z, geo.theta);

    // 3. Downlink Segment (Satellite Relay -> Bob at Ground)
    double wSqB = wSquaredDownlink(w0, geo.z, lambda);
    double eta_down = collection_efficiency(Rground, wSqB, sigma_tr) *
    eta_atmospheric(geo.z, geo.theta);

    // 4. Total End-to-End Success Probability
    double eta_tot = eta_up * eta_relay * eta_down * det_eff;

    // 5. Fidelity Calculation (SNR-based)
    // Probability of noise click within the gating window dt
    double P_noise = 1.0 - std::exp(-rn * dt);

    // Ps: Probability that the click originated from the signal
    double Ps = eta_tot / (eta_tot + P_noise);

    // Final Entanglement Fidelity (1.0 for perfect signal, 0.25 for random noise)
    double Fidelity = Ps * 1.0 + (1.0 - Ps) * 0.25;

    // Display Results
    std::cout << std::fixed << std::setprecision(2)
              << std::setw(10) << DG/1000.0 << " | "
              << std::scientific << std::setprecision(4)
              << std::setw(12) << eta_up << " | "
              << std::setw(12) << eta_down << " | "
              << std::setw(12) << eta_tot << " | "
              << std::fixed << std::setprecision(4)
```

```
              << std::setw(10) << Fidelity << std::endl;
}

int main() {
    double h = 700e3; // Satellite Altitude

    std::cout << "Hybrid Architecture (1 Satellite Relay) - Nighttime Simulation" << std::endl;
    std::cout << "Harmonized Parameters: t_gate = 40ns, r_n = 1500Hz, w0 = 13cm" << std::endl;
    std::cout << "
    ------------------------------------------------------------------------------" << std::endl;
    std::cout << " DG (km)  |   Eta_Up     |   Eta_Down   |   Eta_Tot    |  Fidelity
     " << std::endl;
    std::cout << "
    ------------------------------------------------------------------------------" << std::endl;

    // Loop through various ground separation distances
    for(double dg = 1500e3; dg <= 3000e3; dg += 500e3) {
        runSimulation(h, dg);
    }

    std::cout << "
    ------------------------------------------------------------------------------" << std::endl;
    return 0;
}
```

Listing 6: C++ implementation of the hybrid architecture.