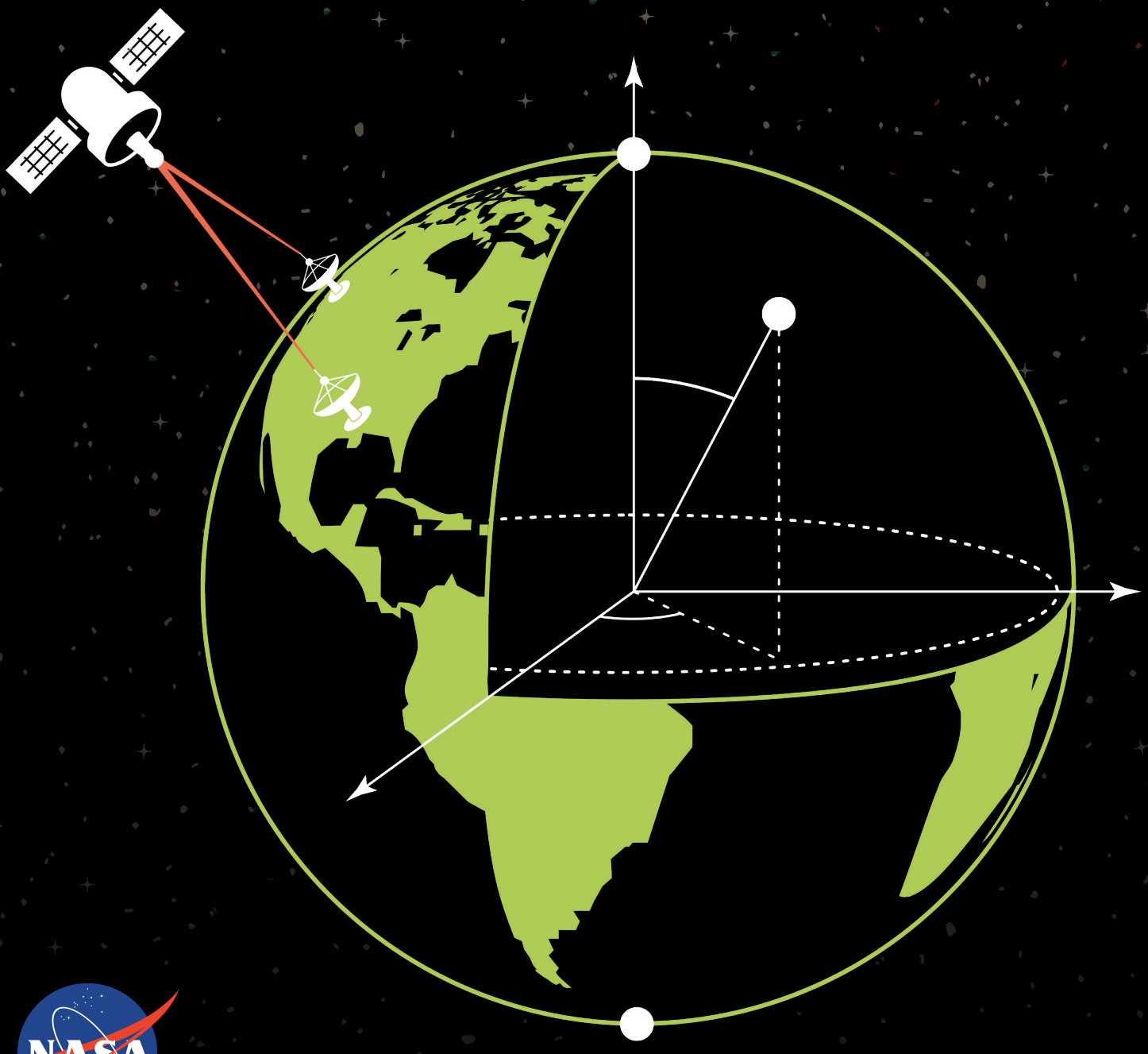
Quantum Communication 101

Henry Semenenko, Sherilyn Wright, Michelle Lollie,
Jefferson Flórez, Matty Hoban, Florian Curchod



NASA

Executive Summary

Our ability to communicate has evolved drastically over the past century with the digitalization of information and advent of interconnected computing devices. Today, there are nearly as many smartphones on the planet as there are humans, all continually exchanging information using complex communication systems. Digital communications also connect personal laptops, smart meters, and more powerful devices such as supercomputers which can be accessed remotely. One of the greatest recent inventions makes use of communications to connect billions of smart devices together in a network of networks known as the Internet of Things. Communication is ubiquitous in modern society; emails and messages are exchanged, and data is accessed and stored remotely on the cloud.

In April 2017, a complex network of eight radio telescopes around the world carefully synchronized in space and time took the first-ever picture of a black hole. This scientific breakthrough would not have been possible without the international collaboration of around 300 scientists from 80 institutes who communicate almost in real time thanks to our modern infrastructure.

Communication extends beyond our atmosphere, enabling space-based technologies from global positioning systems to space exploration. NASA's Voyager 1, launched in 1977, is the farthest spacecraft from Earth and still collects and sends us data while entering interstellar space.

What is quantum communication?

Communication and information processing capabilities are fundamentally tied to the laws that govern the physical systems that are used to transmit and process that information. Communication technologies today rely on *classical* communication, taking advantage of the properties of information carriers that follow the laws of classical physics. These laws are called classical in opposition to *quantum* physics: the physical laws that govern very small systems, such as atoms, electrons, and photons. New quantum rules create new possibilities.

The field of ***quantum communication*** is the study of encoding and transmitting information between distant quantum systems. This relatively new field takes advantage of the peculiar properties of quantum physics, such as superposition, teleportation, and entanglement, which have no classical equivalents. Much like classical communication, quantum communication will rely on light to encode information, which enables fast, low-error communication.

New applications

Last century, we witnessed what is referred to as the first quantum revolution, leading to technologies such as the laser, magnetic resonance imaging (MRI), atomic clocks, and nuclear energy. Our understanding of quantum properties led to mass produced semiconductors, making possible the emergence of classical information technology. As our ability to manipulate individual quantum systems improves further, we are entering a ***second quantum revolution***: the era of quantum information technology.

One of the first applications in quantum communication will be in cybersecurity to enable new methods to secure information. Beyond this, quantum communication is set to enable advancements in computing and metrology. Quantum computing promises to solve problems intractable for its classical counterpart, while quantum metrology will enable measurements at an unprecedented precision.

Space Communications and Navigation (SCaN)

NASA SCaN is a program for all of NASA's space communications activities, which enables both NASA and non-NASA missions. Importantly, it builds and maintains an infrastructure for both near-Earth and deep space communication, which can be utilized for quantum communication.

The SCaN program includes developing technology to send quantum information across its network of ground stations and satellites. In its near-term roadmap, SCaN is working towards a user facility that will enable quantum communication between satellites in low-Earth orbit and ground stations: a quantum testbed. In the long-term, it will enable quantum communication between satellites in medium-Earth orbit and multiple ground stations to enable intercontinental quantum links. Central to the SCaN mission is the distribution of quantum entanglement, which will enable quantum repeaters for long-distance quantum communication and the applications that can be built from it. Through an international collaborative effort, the SCaN testbed will aid the development of quantum technologies to accelerate the progress towards new quantum applications.

Roadmap

NASA's SCaN roadmap aligns with, and provides critical infrastructure support for, the National Quantum Initiative (NQI) (announced in August 2018 by the United States Government) as well as decades of investments in quantum information science (QIS) of the National Science Foundation (NSF), Department of Defense (DoD), Department of Energy (DoE), and other government agencies. In particular, the NSF recently announced a $5.1M Center for Quantum Networks aimed at architecting the quantum internet. It also follows a worldwide investment in QIS over the last few years. Examples include the $1.1B Quantum Technology Flagship in Europe and the $11B Chinese National Laboratory for Quantum Information Science. Important industrial investments are also being made by large corporations such as IBM, Google, Intel, Honeywell, Cisco, and Microsoft.

Who is this booklet for?

This booklet on quantum communication targets both the wider audience interested in exploring the topic for the first time and experts wishing to discover NASA's SCaN roadmap. We avoid equations as much as possible, though our reader will need to engage at a high level with a small number of mathematical concepts. The introductory chapters provide the necessary background on key concepts specifically related to quantum communication and are not to be considered comprehensive. Later chapters explore in more detail communication links and networks, together with their technological challenges. Finally, we discuss the future of quantum communication and the exciting new applications that the field will enable.

Contents

1 Introduction 1

Quantum information . . . 1
Challenges . . . 2
Applications . . . 2
The quantum internet . . . 3

2 Quantum Information 4

Systems for quantum communication . . . 4
The quantum bit, or qubit . . . 4
Quantum measurement . . . 6
Heisenberg's uncertainty principle . . . 7
No-cloning theorem . . . 7
State transformation . . . 8
Quantum entanglement . . . 8
Quantum computing . . . 9

3 Quantum Light 11

What is light? . . . 11
Generating light . . . 12
Encoding quantum information . . . 15

4 Components 18

Single-photon sources . . . 18
Entanglement generation . . . 21
Single-photon detectors . . . 22
Supporting equipment . . . 26

5 Quantum Links 28

Channel errors . . . 28
Fiber links . . . 29
Free-space links . . . 30
Satellite quantum links . . . 31
Satellite link architecture . . . 33
Launching satellites in the real-world . . . 34

6 Quantum-Enhanced Security 36

Quantum cryptography . . . 36
Encryption . . . 37
Distributing shared keys . . . 38
The threat of quantum computing . . . 40

Quantum key distribution . . . 40
Device-independence . . . 42
Recent developments . . . 43
Post-quantum cryptography . . . 44
NASA's SCaN . . . 44

7 Quantum Metrology **46**
Limits of measurement . . . 46
Quantum parameter estimation . . . 49
Atomic clocks . . . 50
Metrology for communication . . . 51

8 Quantum Networks **53**
Entanglement distribution . . . 53
Networking . . . 58
Quantum network developments . . . 59

9 The Quantum Internet **64**
Distributed quantum sensing . . . 64
Distributed quantum computing . . . 67
Delegated quantum computing . . . 69
Quantum cryptography . . . 72

10 Summary and Open Problems **74**

Further Reading **77**

Abbreviations **78**

Glossary **80**

References **84**

1 Introduction

At a high level, the text I am typing now is stored in electric charges in my laptop's memory, then a radio transmitter will encode my text somewhere within some radio waves that are sent to a router. The router receives the radio waves and transmits my text via electrical currents in a copper wire connecting to a port, where the currents are converted to infrared light, which is sent down glass fiber to the outside world.

For the words that start in my laptop to successfully end up as pixels on your screen, the information corresponding to this text must be *encoded* in the properties of many different particles and waves. It is important to note that information is not synonymous with the particles or waves that carry it. It is something more abstract than a particular physical thing, such as an electrical wire, a radio wave, or a charge in a capacitor.

Conventionally, information stored in a physical system is described in terms of *binary digits*, or *bits*, which can take the values 0 or 1. Different classical systems store information in different ways. In a capacitor each bit is encoded in its charge state: it is charged or not. For light there are many ways we can store bits. For instance, the *amplitude* of light can encode bits, where 1 corresponds to a light signal that is bright, and 0 corresponds to a less bright signal. The receiver of the light signal would then convert the brightness back into electrical signals to retrieve the information. Whatever the property used to carry the information, long distance communication is performed using light since it is fast and does not interact too strongly with its environment.

One central feature of classical information, and something that is implicit but is worth stating for clarity, is that the bits carried in a classical system have definite values: 0 *or* 1. Information can get corrupted and changed, but it will only be changed to another set of definite values. Furthermore, these definite values of information can be read and copied arbitrarily to other physical systems.

Quantum information

While classical information can be encoded in systems that behave according to the laws of classical physics, the picture changes drastically when encoding information in systems whose behavior is described by quantum physics. When encoding information in the properties of a quantum particle, such as a photon, the laws of quantum physics apply – laws that are notoriously counterintuitive for us humans, whose experience of the world is well described by classical physics.

Quantum information has several interesting properties that have no classical counterpart. For example, the units of quantum information may not have definite values. Instead of bits, we now have quantum bits, or ***qubits***. The state of a qubit can correspond to definite values of 0 or 1 as in classical information but can also be in a ***superposition*** which is a combination of 0 *and* 1. While in superposition, a qubit can be described by many possible data values simultaneously. However, only when an observation, or measurement, is made to read the state of a qubit do we get a specific value. Before the measurement, it is not possible to say which value will be obtained from measuring a qubit. In other words, quantum physics can be fundamentally unpredictable.

Quantum systems can also exhibit *entanglement*, a property whereby the quantum information of multiple particles is correlated in a way that does not respect their location. For their experiments to prove that nature does indeed behave in this way, Alain Aspect, John F. Clauser, and Anton Zeilinger were awarded the 2022 Nobel Prize in physics[1]. Entanglement has no analogue in classical physics or classical information systems, and represents what Erwin Schrödinger, one of the founding fathers of quantum physics, described[2] as "*the characteristic trait of quantum mechanics*." This makes it an essential resource in quantum communication and other applications in which we seek quantum advantage.

Challenges

Quantum information is difficult to prepare, store, manipulate, and retrieve. Quantum communication makes use of physical systems that behave according to the laws of quantum physics, which are typically at the atomic and sub-atomic scale. Therefore, the level of control and precision required is very high and the tolerance to noise is low. This opens a new range of technological challenges, collectively called the *quantum engineering* challenge.

One vitally important distinction between classical and quantum information is that quantum states cannot be copied; a fact known as the *no-cloning theorem*. In classical information systems, signals can be amplified to counteract the effect of information being lost to the environment as they travel through a network. A major step forward in the development of quantum networks will therefore be the reliable and long-distance distribution of quantum entanglement, which will enable quantum repeater technology to overcome distance limitations.

Applications

While some nascent quantum communication systems exist today, realization of their full potential will require significant technological advances, which engineering teams around the world are working on at pace.

Short distance and point-to-point implementations include prototype quantum key distribution (QKD) networks, some of which span metropolitan areas, and high-precision clock synchronization. Distributed quantum sensing and quantum computing networks, on the other hand, will only be possible with more mature, and thus future, quantum technologies such as quantum repeaters and large-scale entanglement distribution.

Metrology, the field of measurement, has already seen improvements in sensing devices by exploiting quantum phenomena. By understanding the fundamental limits of noise, quantum systems are being used to make precision measurements not previously possible. For example, quantum states of light are being exploited in LIGO, a large-scale experiment run by CalTech to measure gravitational waves with two observatories in Hanford, Washington and Livingston, Louisiana, with a vastly improved detection rate[3].

Small-scale quantum computers are now being developed at many private sector companies, government laboratories, and university research facilities, following tens of billions of dollars of

investment in the past decade or two. These devices exploit the properties of quantum physics, including superposition and entanglement, to perform certain computations faster than conventional computers using classical information. They are expected to solve certain problems that are intractable for their classical counterparts in fields such as physics, Earth science, materials science, chemistry, optimization, artificial intelligence, and cybersecurity. It is suggested that to achieve sufficient scale to tackle the largest problems, quantum computers will be built in spatially separated locations and exchange quantum information. Such quantum computers will need their own quantum communication channels, or *quantum links*. Given the potential value of the computations conducted by these devices, it may be essential for these links to be capable of hiding the information that the computers perform operations on, for reasons of commercial privacy, or national security.

The quantum internet

The end goal of quantum communication is what many refer to as the ***quantum internet*** through which we will seamlessly distribute quantum information across many individual quantum networks for sensing, processing, and securing data. Along the way, much work needs to be done to develop state-of-the-art components for generating, manipulating, and detecting quantum signals. New network nodes must be built, including space-based nodes that require lightweight satellites and advanced tracking technology. Ultra-low loss optical fiber and quantum repeaters must be developed to extend the reach between nodes.

At the forefront of a number of these advances is NASA's SCaN, who are also one of the leaders in developing long-range entanglement distribution, an essential requirement in future quantum networks. This booklet makes heavy reference to the Workshop on Space Quantum Communications and Networks that was held by NASA in September 2020[4]. A final report is available through NASA's website which provides a more in-depth discussion of the topics in the field of quantum communication.

2 Quantum Information

To understand quantum communication and its applications, we must first introduce the essential concepts of quantum information. In this chapter we explore the quantum bit, or qubit, as well as what can be done when we have access to multiple qubits. We explore the exclusively quantum property of entanglement, which is fundamental to many quantum communication functionalities and applications of the future. Topics include transformations on qubits (how to manipulate them to encode information), the no-cloning theorem (which both forbids the amplification of quantum signals but also opens new possibilities for secure communications), quantum measurements and their probabilistic nature, the uncertainty principle, and the disturbance of quantum states. Finally, we briefly introduce the field of quantum computing which will play a vital role in future quantum communication networks.

We remind the curious reader that this is a high-level, brief, and communication-focused introduction to the broad field of quantum information. Today, this field is covered widely and exhaustively in dedicated books which can be found in the Further Reading section for those who wish to read in more depth.

Systems for quantum communication

The basic principle of information communication is the same whether it is classical or quantum; one prepares a system in which information is encoded and sends it over a network where it is routed to the intended recipient who measures the system to retrieve the information. Although the principle is the same, every part of what we just described changes when using quantum systems as information carriers. The general setup for communicating quantum information is demonstrated in Figure 2.1. In this chapter, we explain the fundamental concepts needed to describe quantum systems, how they are manipulated to encode information, and how to measure the systems to "read" the information they carry. Reliably transmitting quantum information, or being able to send quantum systems over distances without losing their information, is one of the main challenges of quantum information science and the subject of dedicated chapters.

The quantum bit, or qubit

"Information is physical."

Rolf Landauer

The *bit* is a fundamental notion of classical information. At the most elementary level, information can be written as a string of bits, a bitstring, of 0s and 1s, which *represents* its content. For example, the letter 'a' is encoded into the bitstring 01100001 using the ASCII binary code. Writing, or encoding, a bit of information in a physical system is achieved by modifying a specific property of the system that will represent that bit of information. For example, our computers use electrical signals to represent information where we encode the bit value 1 if the voltage is high and 0 if the voltage is low. By

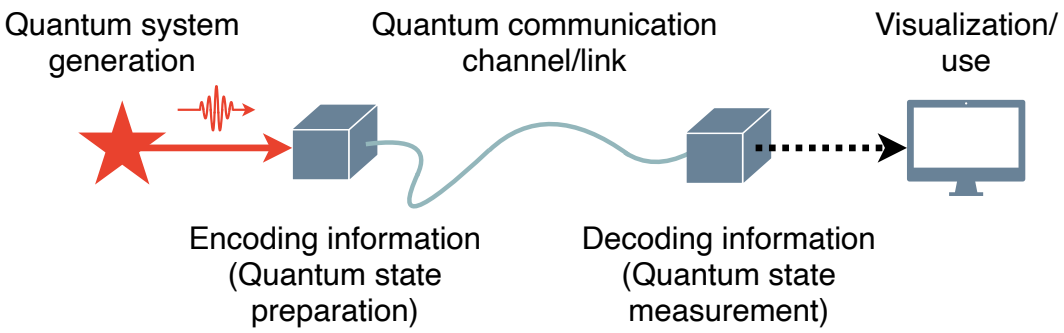


Figure 2.1: Basic principle of quantum information communication.

reading, or measuring, that physical property one can then retrieve the bit of information that was stored. For communication, a very convenient physical system is light, which travels fast and weakly interacts with its environment. Modulating the properties of light, hence encoding information in it, allows us to reliably transmit information over large distances. What often goes without saying with a classical bit is that it is either 0 or 1; an electrical voltage is either high or low. This agrees with our intuition of the world and stems from the physical properties of classical systems that take *definite* values.

Quantum information builds on an analogous fundamental concept: the quantum bit, or ***qubit***. Like classical bits, a qubit can be described using the values 0 and 1, which are now represented by the *states* $|0\rangle$ and $|1\rangle$ to differentiate from their classical counterparts. The difference comes from the behavior of systems that are described by the laws of quantum physics and hence the type of information that they can carry. We have enclosed the values 0 and 1 between a vertical line and angled bracket to represent a quantum state. This notation is called Dirac, or bra-ket, notation and is widely used in quantum physics.

Unlike bits, qubits can exist in a ***quantum superposition*** state where the state is not definitely $|0\rangle$ or $|1\rangle$ but instead must be described by a combination of the two. To write the state of a qubit in superposition, we use the sum $\alpha|0\rangle + \beta|1\rangle$ where α and β are numbers that describe the specific composition which, in general, are complex numbers.

The qubit $\alpha|0\rangle + \beta|1\rangle$, which is commonly labeled $|\psi\rangle$, can be represented by a point on the surface of a sphere, as shown in Figure 2.2. This sphere of unit radius, known as the Bloch sphere, is very useful to visualize a qubit $|\psi\rangle$, in terms of angles θ and ϕ. In fact, these angles are explicitly connected to the coefficients α and β. For example, if $\theta = 0°$, $\alpha = 1$ and $\beta = 0$, resulting in $|\psi\rangle = |0\rangle$. The state $|0\rangle$ is in the north pole on the Bloch sphere, while $|1\rangle$ is diametrically opposite to it. All kinds of operations over the qubit $|\psi\rangle$ can be understood as a rotation, projection, or contraction on the Bloch sphere, making it an important tool to understand qubits. We have included the Bloch sphere here for reference to the reader to help visualize quantum information processing.

Generally, quantum systems are small objects such as electrons, photons, or atoms, whose quantum properties are hard to observe in macroscopic objects. The polarization of a photon is an example of a physical property that can be used to carry quantum information. As quantum systems behave differently to classical ones, qubits allow for information to be encoded, manipulated, transmitted,

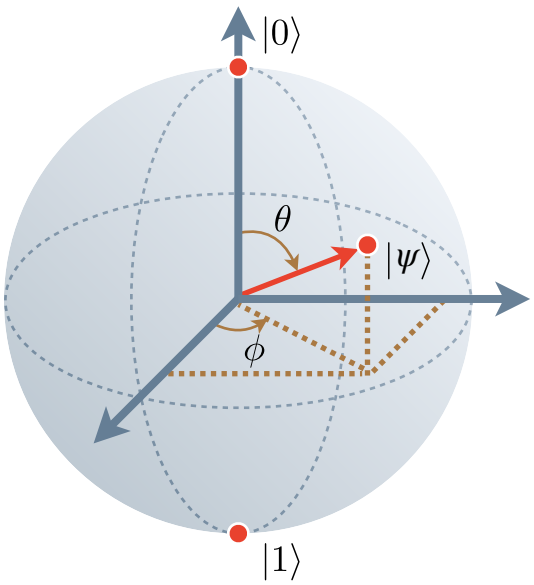


Figure 2.2: Graphical representation of a qubit, $|\psi\rangle$, on the Bloch sphere. The quantum states, $|0\rangle$ and $|1\rangle$ located at diametrically opposite points from each other are also shown.

and read in new ways that offer new possibilities in information processing and communication. The objective of quantum information science is to take advantage of these new possibilities.

Quantum measurement

A measurement is the process of reading a particular property of a physical system, allowing us to retrieve the information encoded in it. As such, when we make a ***quantum measurement***, we are mapping the quantum information in the qubit state to classical information described by bits and the outcome of the measurement has a definite value. This implies that, although the value of a qubit was undetermined before the measurement, the qubit is *projected* to a determined value after a measurement. This mapping between a qubit state and a classical bit is therefore intrinsically probabilistic, which is unlike classical physics.

For a qubit in a superposition state $\alpha\,|0\rangle + \beta\,|1\rangle$, the numbers α and β relate to the probabilities that, when the qubit is read using a measurement, the result will read 0 or 1. The way that those probabilities are computed is given by the *Born rule*: one of the fundamental principles of quantum mechanics. Receiving an unknown qubit, $\alpha\,|0\rangle + \beta\,|1\rangle$, one can for example measure whether the state is $|0\rangle$ or $|1\rangle$ (called measuring in the computational basis). Born's rule, in this case, tells us that this state has probability α^2 of giving outcome 0 and $\beta^2 = 1 - \alpha^2$ of giving outcome 1. In the extreme case where $\alpha = 1$ and $\beta = 0$, i.e., the qubit state is $|0\rangle$, the outcome 0 is obtained with probability $\alpha^2 = 1$ as the state is indeed $|0\rangle$.

Certain quantum measurements have intrinsically unpredictable outcomes, which is fundamentally different from classical randomness which always stems from a lack of *knowledge*. For example, the outcome of a coin toss appears random as we do not accurately know the starting position and all forces acting on the coin. It would be natural to question how a framework that is intrinsically random can be useful for processing information. Randomness plays a vital role in many applications and

has immediate applications in both cryptography and computer science. This quantum randomness, or unpredictability, is what is harnessed by quantum random number generators and is a critical foundation enabling new cryptographic primitives.

Another aspect of a qubit is that, when measured, a superposition state gets *projected* to the well-defined states corresponding to the outcome that was obtained; the state the qubit was in before the measurement is lost. For example, if we have encoded the polarization of a photon as the qubit $\alpha |0\rangle + \beta |1\rangle$ and we measure to obtain the outcome 0, the state of the polarization of the photon after the measurement is now $|0\rangle$; the information encoded in α and β has been erased. By making the measurement we have influenced, or *disturbed*, the state of the system.

This invasive role of the observer, or of the measurement process, does not happen in classical physics. This property has also been leveraged in quantum cryptographic protocols making it possible to detect the disturbance that an eavesdropper introduces in a communication channel.

Heisenberg's uncertainty principle

Heisenberg's uncertainty principle is a fundamental concept in quantum physics that also has no classical analogue. It states that there is a fundamental limit to the precision with which one can measure certain pairs of physical properties at the same time. More precisely, for properties that are said to be complementary, the more accurately one property is measured the less accurately the other can be known. For example, the position and the momentum of an electron cannot be known simultaneously with arbitrary precision; measuring the position accurately will mean obtaining a large uncertainty when measuring the momentum. Numerous other properties apart from position and momentum cannot be measured simultaneously.

Mathematically, denoting the position of the particle with x and its momentum with p, the uncertainty principle takes the form $\Delta x \Delta p \geq \hbar/2$, where Δ denotes the uncertainty of the given property to be measured. The reduced Planck constant $\hbar$ is a fundamental value limiting the joint precision that can be obtained. The uncertainty principle is especially relevant in the field of metrology, as we will discuss in Chapter 7, where it provides a fundamental limit on measurement precision.

No-cloning theorem

The probabilistic nature of the measurement process, together with the state disturbance of measurements, leads to the following interesting observation. For a classical bit, it is possible to completely reconstruct the information from a single measurement as there are only two possible values. We can create two copies of the bit using the measured outcome.

However, if given a single qubit (a single physical system, one photon for example), a single measurement does not yield enough information to reconstruct the state and, furthermore, the act of measuring erases the state. Even given many identical copies of qubits in the state $\alpha |0\rangle + \beta |1\rangle$, one could perform the measurement on each copy and still only provide an *estimate* of the true state from the frequency of the outcomes. In other words, one cannot *exactly* determine the state of a single qubit in an unknown state.

This observation stems from a more profound property of quantum mechanics; given a qubit in an unknown quantum state, it is impossible to make even a single copy of it. This result is known as the ***no-cloning theorem*** and implies that quantum signals cannot be amplified at a fundamental level. As an example, we saw above how it is not possible to use the outcome of a single measurement to exactly reconstruct the state of a qubit. Therefore, we could not simply measure the state of a qubit and then create two copies. However, this is only one possible strategy. Perhaps we could construct a more complex process with different operations to copy a qubit. The no-cloning theorem tells us that there is no process allowing us to end up with two copies of an unknown quantum state. As copying qubits is forbidden, it is not possible to use amplification techniques that are commonplace in modern communication networks. This has important consequences for the distance over which quantum information can be transmitted and is one of the main challenges of quantum communication.

State transformation

We have introduced quantum systems that carry quantum information, and how measuring them allows us to retrieve that information. Analogous to signal modulation in classical communication, one also performs transformations on quantum states, for example to encode information in them. Transformations on qubits can be seen as quantum gates which are conceptually similar to the classical computing case.

Classically, the only non-trivial transformation on a single bit is the NOT gate which flips the bit value, i.e., the 0 and the 1 are interchanged. For quantum states, and contrary to the classical case, in addition to the NOT gate there is now a continuum of possible quantum transformations. Instead of simply interchanging $|0\rangle$ and $|1\rangle$, one can now transform $|0\rangle$ to any superposition $\alpha\,|0\rangle + \beta\,|1\rangle$ (and specify the action on the state $|1\rangle$). Contrary to measurements, transformations are also reversible: they do not erase information.

One example operation that is commonly used in quantum information is the Hadamard operator. When applied to the state $|0\rangle$, the qubit is transformed into the superposition state $1/\sqrt{2}(|0\rangle + |1\rangle)$, while a qubit in the $|1\rangle$ state becomes $1/\sqrt{2}(|0\rangle - |1\rangle)$. Applying the Hadamard operator again would return to the original state, reversing the operation. For example, a qubit in the state $1/\sqrt{2}(|0\rangle + |1\rangle)$ would be transformed back to $|0\rangle$. It is not always the case that an operator can reverse itself like this. However, for the operations we often care about in quantum information, they can be reversed by another operation.

Quantum entanglement

We will now see how the possibility for quantum states to be in a superposition state leads to the phenomenon of ***quantum entanglement*** of multiple qubits. This is one of the most spectacular properties of quantum systems and is an incredibly valuable resource for quantum communication.

Bitstrings are used in classical information to combine individual bits to represent more complex data. Two classical bits can have one of four values: 00, 01, 10, or 11. Systems of multiple *qubits* can be described in a similar way where we concatenate the two states. For example, two qubits

may have the state $|01\rangle$ where the first qubit is in the $|0\rangle$ state, while the second is in the $|1\rangle$ state. However, just as a single qubit can be in a superposition state, multiple qubits can be in a *collective superposition* state. This allows combinations of states like $|01\rangle + |10\rangle$ which is an example of an *entangled* state.

As this is a superposition state, the value of each qubit before it is measured is not determined; we will receive a value of 0 or 1 at random for both the first and second qubit. However, while the value for each *individual* qubit is random, the values of both are *anticorrelated*: when we compare the results, we find they are always opposite. If we find that the first qubit is 0, the second must be 1!

Two classical bits might have the value 01 where the individual bits are anticorrelated. However, their values are well defined. The first bit is always 0 and the second always 1. To compare with the entangled case, the values will always be anticorrelated but the values for each will be random.

Quantum entanglement is especially surprising when the two qubits are carried by two physical systems. Imagine that two photons are in an entangled state but are far apart from each other. We could measure the first photon and, for example, find the outcome 0. The *projection* of the state induced by the measurement of the first photon then implies that the state of both photons now is $|01\rangle$. In other words, the state of the second photon is now well defined and would now yield the outcome 1 with certainty if measured. The state of the second photon, which was undetermined before, appears to have been changed by measuring the first photon, despite them being far apart!

When this phenomenon was first proposed, it was famously described as "*spooky action at a distance*" by Albert Einstein[5]. Ultimately, it started a line of work intending to demonstrate that our universe is indeed quantum, which culminated with a groundbreaking result by John Bell[6]. This result, known as Bell's theorem, provided a framework in which we could measure quantum correlations in entangled systems and show that these could never exist under the laws of classical physics. In 2022, Alain Aspect, John F. Clauser, and Anton Zeilinger were awarded the Nobel prize in physics for their experiments testing Bell's theorem using entangled photons[1].

Quantum computing

One extremely promising quantum information technology is quantum computing. Quantum computers process quantum information encoded in qubits to perform certain computations faster than can be done with classical computers. A very impressive aspect of quantum states is the amount of information that can be "contained" within the state. As we have seen, a single qubit state $\alpha|0\rangle + \beta|1\rangle$ can have α and β take on any value between 0 and 1 – in other words, the values of α and β are continuous. Two qubit states are superpositions between four basis states: $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, that is, a continuous range for four different numbers. An n qubit state is a superposition of 2^n terms, i.e., 2^n such numbers. This means that even for 300 qubits, there are many more numbers in the n qubit state than the estimated number of atoms in the observable universe! Nature therefore seems to handle this vast amount of information when those systems are generated, transformed, or interact. The hope of quantum computing is to be able to take advantage of this huge amount of information handling power to perform computations: to compute like Nature. This argument can also be used the other way around; to simulate nature, which at a quantum level

contains such a vast number of possible states, we will need the same type of power. To solve chemistry or condensed matter problems, for example, one will need quantum systems to simulate other quantum systems. In fact, it is already known that classical computers very quickly reach their computational limit, even to simulate the behavior of relatively small molecules. This is particularly clear when the number of possible states is very large due to the number of possible configurations of electrons interacting within and between atoms.

There is an intense debate around whether today's quantum computers can demonstrate a ***quantum advantage***; that is to say, can today's quantum computers perform any computation that would not be possible even on the most powerful classical computers available? One of the major obstacles for the advent of useful quantum computers – that not only beat their classical counterpart at some task, but at a useful task – is their scaling. If quantum computers can be built at scale, and if they can process many qubits reliably, they are predicted to be useful in a wide range of problems that are otherwise intractable for their classical counterparts. Examples range from material and pharmaceutical discovery through chemical simulation to financial predictions, natural language processing, modeling climate change effects on the complex Earth system, and cybersecurity. Quantum computers are currently being scaled up rapidly by a growing number of companies, government laboratories, and university research departments around the world.

Useful quantum computers will need to manipulate large numbers of physical qubits, to provide sufficiently many logical qubits once error correction is considered. Quantum error correction is a technique used to protect quantum information from noise by using several physical qubits to encode information into a logical qubit. By spreading the information over many physical ones, it is possible to correct errors at the logical level by applying correction operations to the physical qubits. One promising way forward for the scaling of quantum computers is to connect them to combine their respective qubits, which will require quantum communication links. More generally, quantum communication links will be the backbone of future quantum networks which connect quantum computers, repeaters, and other quantum technologies. While quantum computing is out of scope for this booklet, we invite the reader to explore dedicated material in the Further Reading section to learn more.

3 Quantum Light

Light is fundamental in global communication networks. Optical signals generated by lasers and distributed through fibers made from glass form the backbone of the Internet. The speed of light enables communication across countries and continents with almost no delay. Furthermore, light does not easily interact with other light or external fields allowing for low noise communication over very long distances.

Our understanding of light has changed dramatically over the past century and has since become fundamental in the current quantum revolution. In this chapter, we will explain the distinctive quantum properties of light in terms of its constituent photons and their statistics. We will see how we can use them to encode quantum information and how light will form the basis of quantum communication.

What is light?

Light is a wave with all the properties of classical waves, like ocean or sound waves. Light waves can interfere to reinforce or cancel each other, diffract around obstacles or after an aperture, and refract (bend) when passing between two different transparent materials. However, unlike other waves, light can travel through empty space, such as most of the outer space between Earth and the stars in the universe. This transmission in a vacuum is possible because light is an oscillating wave with no mass and, consequently, needs no particles to propagate. Instead, light propagates as an electromagnetic wave, as shown in Figure 3.1, composed of electric and magnetic fields oscillating perpendicularly to each other and to the propagation direction. Light waves through an electromagnetic field travel at a constant speed – 299 792 458 meters per second in vacuum.

A wave is characterized by the distance between its peaks or troughs, known as the wavelength, and the rate at which the peaks oscillate in the propagation direction, which is the frequency. As light travels at a constant speed, wavelength and frequency are intrinsically linked – light with a long wavelength has a low frequency and vice versa. We experience a change in light frequency as a

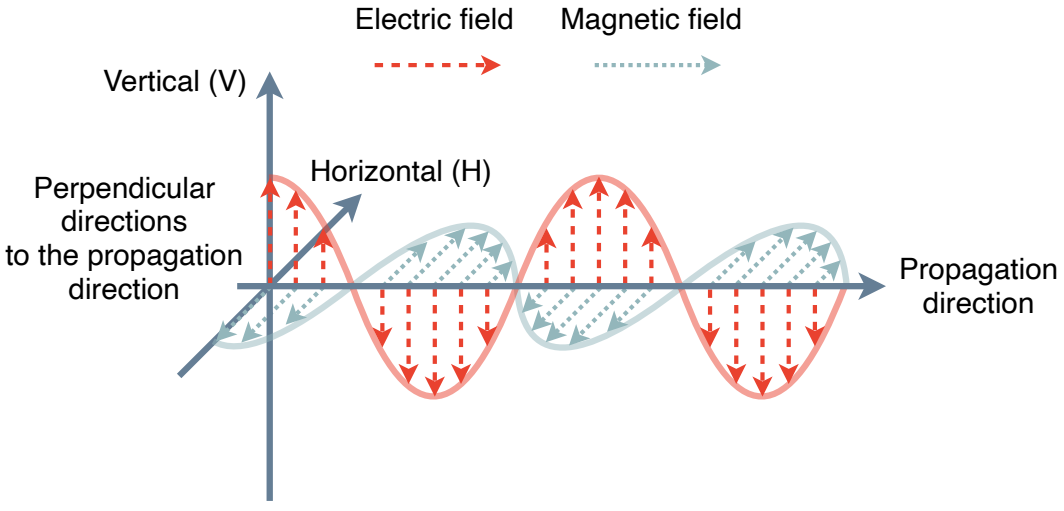


Figure 3.1: Linearly polarized electromagnetic wave traveling along the propagation direction.

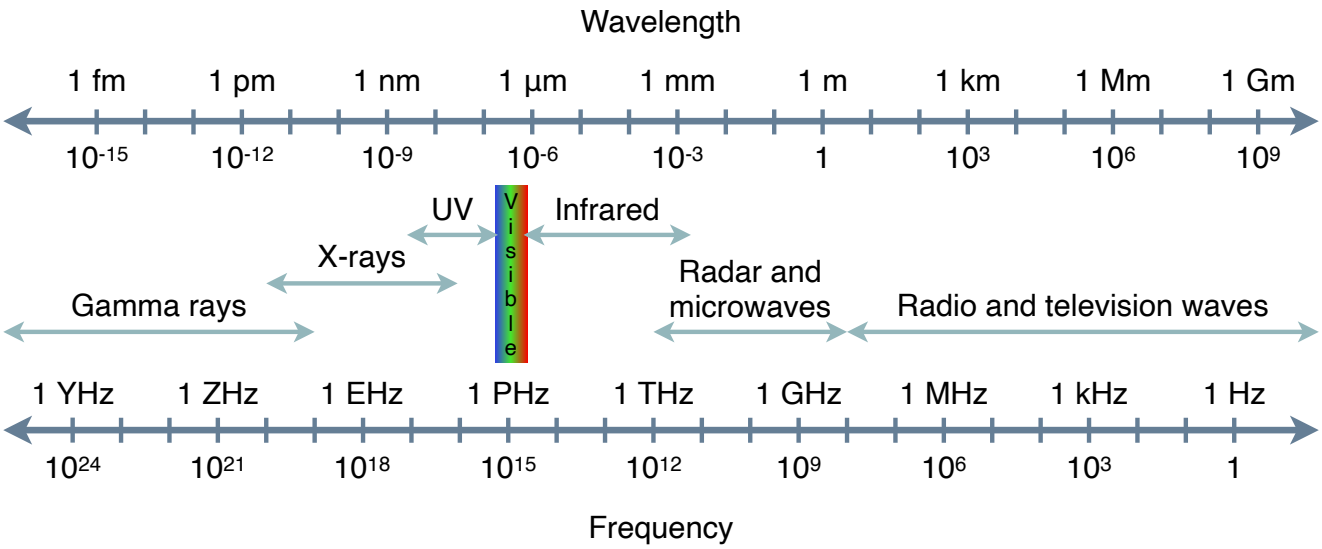


Figure 3.2: Electromagnetic spectrum showing frequency and wavelength. The spectrum is broadly separated into seven regions.

change in color in the light we can see; blue light has a higher frequency than red light. However, the electromagnetic spectrum is much broader than this visible range. Anything from gamma rays to radio waves are also electromagnetic waves and are also light, although we cannot see it with our eyes. An overview of the electromagnetic spectrum is shown in Figure 3.2, including the ultraviolet (UV), visible, and infrared regions.

Where our understanding of light diverges from a classical wave description is its discrete energy composition. Light consists of indivisible energy packets, called photons, that we picture as light particles. The idea of the photon was formally introduced in 1905 when Albert Einstein proposed that electrons ejected from an illuminated metallic surface result from the absorption of photons, or quanta of energy. At the time, the photoelectric effect disagreed with the leading theory of light that described wave energy uniformly distributed in space. According to this theory, atoms would take a few minutes to absorb the dispersed wave energy and allow electrons to leave the metal. In contrast, experiments showed almost no delay once the light source was turned on, suggesting that the wave energy concentrates in clusters – photons – that are readily absorbed by electrons. Furthermore, where efforts to observe the photoelectric effect in metals using bright sources of visible or lower frequency light have failed, the use of even dim UV light sources has succeeded in ejecting electrons from the metal. This observation suggests that the photon energy is proportional to the light frequency – the higher the frequency, the higher the photon energy. Since UV photons are higher in frequency, they provide enough energy to eject electrons while light of lower frequency does not, regardless of the light intensity.

Generating light

As much as the study of light has led to revolutionary discoveries, the impact of generating artificial light has been profound. Throughout the 19th century, it was shown that passing an electrical current through certain materials, such as carbon, would cause them to glow. This discovery would eventually

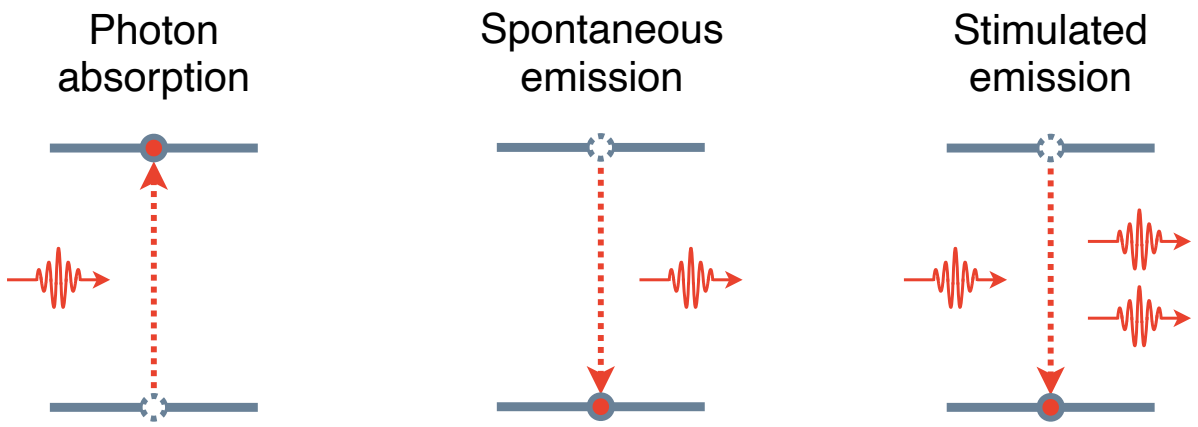


Figure 3.3: Light interaction with electrons through absorption or emission. An electron that absorbs a photon moves to a higher energy level and emits a photon when it decays to a lower energy level. A photon can stimulate the emission of a photon from an excited electron.

lead to the incandescent bulbs that we use today, although they are being quickly overtaken by more energy efficient technologies such as compound fluorescent light and light-emitting diode (LED) bulbs, which use far less energy to light a room by taking advantage of other quantum mechanical effects.

Early in the 20th century, quantum mechanics was born from energy quantization ideas developed by Max Planck and Niels Bohr, leading to a new understanding of the atomic world. Atoms became complex structures with electrons occupying discrete energy levels. This model also postulates that an atom emits a photon when one of its electrons transitions from a higher to a lower energy level, with an energy equal to the difference between these two levels. Conversely, when an atom absorbs a photon, one of its electrons transitions from a lower to a higher energy level, as shown in Figure 3.3, where the photon energy again matches this energy difference. This is the underlying explanation for the photoelectric effect – if the light incident on a metal does not have enough energy in each photon, the electrons will not be excited enough to leave the metal.

Lasers

Around the 1960s, physicists discovered how to manipulate electrons undergoing these energy transitions in atoms – or molecules – to get bright, collimated light from a device that we call a ***laser***. Inside a laser, electrons are mainly at a high energy level within their respective atoms thanks to an external energy source. When a photon encounters one of these excited atoms, it triggers the production of an identical photon through a process known as stimulated emission, shown in Figure 3.3. These two photons stimulate the production of more photons in nearby atoms, all moving in the same direction, causing a cascade. To enhance this effect, atoms are enclosed by two mirrors facing each other, creating an optical cavity where photons bounce multiple times. This is shown in Figure 3.4. One of the mirrors is semi-transparent and allows a fraction of the bouncing photons to escape the cavity, which becomes the light emitted by the laser. This way of generating light is known as light amplification by stimulated emission of radiation, from which the acronym laser was coined.

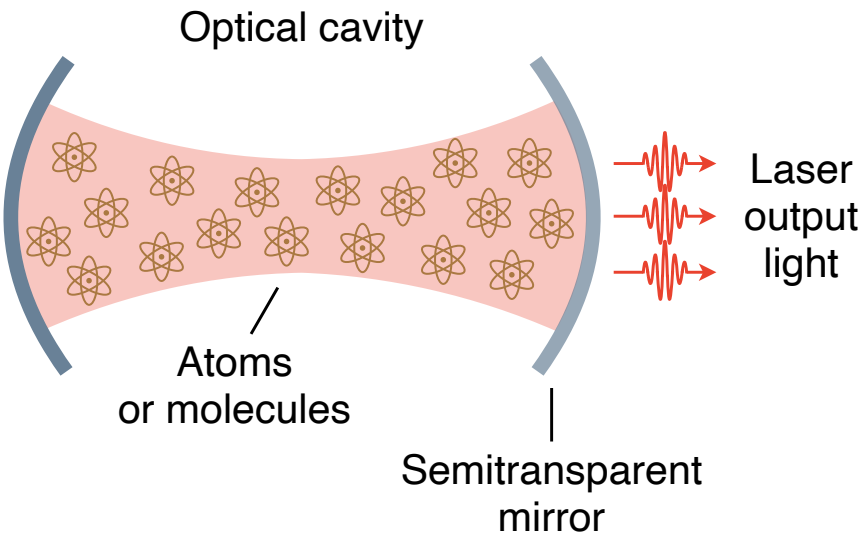


Figure 3.4: A laser in which atoms or molecules are stimulated between mirrors to emit a bright, collimated beam of coherent light.

Coherent light

In a light bulb, atoms in the filament vibrate and collide randomly with each other, exciting their electrons to high energy levels and emitting light of many frequencies in all directions in the process. In contrast, atoms in a laser are stimulated together and emit highly monochromatic and unidirectional light synchronously as a result.

There is a correlation in the photon emission times within a laser, which leads to atoms radiating light simultaneously; we say this simultaneous emission is ***in-phase***. Physicists use the adjective ***coherent***, as in optical coherence, to describe light that has this in-phase property. This optical coherence exhibited by a laser manifests, for example, in diffraction and interference experiments. However, other light sources like light bulbs also exhibit these optical phenomena. Therefore, a precise definition of coherence was introduced in 1963 by Roy J. Glauber to account for the distinctive properties of lasers.

Glauber introduced a collection of functions to compare light at different points in space and time. The specific function we are interested in here is the second-order correlation function that is denoted by $g^{(2)}(\tau)$. This function describes the likelihood of detecting a photon at time t and a second photon at time $t + \tau$. The time that we are most interested in is when $\tau = 0$. Measuring the correlation function allows us to separate light into three distinct categories. In the case of light from a light bulb, photons are produced chaotically, and we find that $g^{(2)}(0) > 1$. We describe light with $g^{(2)}(0) > 1$ as ***bunched*** light. For light from a laser, we find that $g^{(2)}(0) = 1$ which is the condition for light to be ***coherent***. Finally, let us consider the correlation measurement of a single photon. Intuitively, we find that $g^{(2)}(0) = 0$; as we have only a single photon, we could not measure a second photon. We describe light where $g^{(2)}(0) < 1$ as ***anti-bunched***, and this is a condition for light to behave quantum mechanically.

A common method to measure $g^{(2)}(\tau)$ is shown in Figure 3.5 and is known as a Hanbury-Brown-Twiss experiment after its inventors. A light source is split by a device known as a beam splitter which

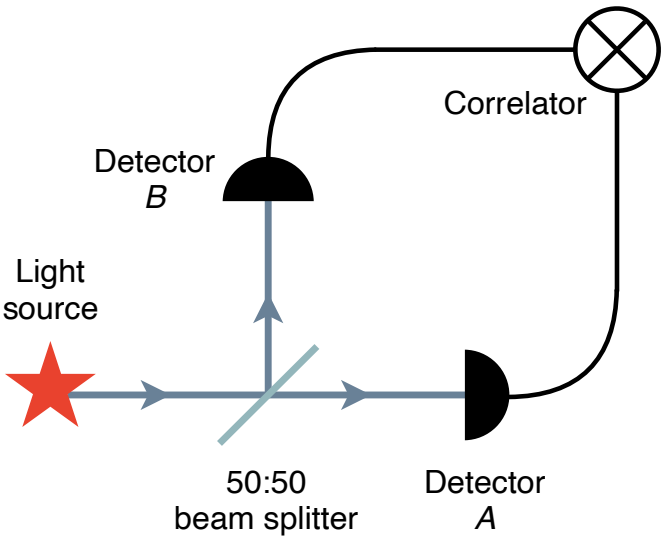


Figure 3.5: Hanbury-Brown-Twiss experiment to study coherence of a light source. Light is split with a beam splitter into two paths which are measured using a detector and the outcomes compared with a correlator.

reflects half of the light and transmits the rest. We can then measure the light using two detectors and record the correlation between the two paths.

Encoding quantum information

A common method use light to encode information for communication is to use the brightness of a light pulse. For example, a bright light pulse may encode a '1' while a dim light pulse encodes a '0'. However, there are other properties of light that can be used to encode information. To conclude this chapter, we will introduce a few properties of light that will be essential in quantum communication and describe how a single photon can be used as a qubit.

Polarization encoding

Polarization of light is a phenomenon that has been present in applications for centuries. Nowadays, polarized sunglasses are commonly used to avoid glare from reflective surfaces and polarizers are a critical part of computer displays.

Considering light as an oscillating electromagnetic wave, we define the polarization of light as the direction in which the electric field oscillates. In Figure 3.1, the electric field oscillates along the vertical direction perpendicular to the propagation direction. Therefore, we say that this wave is linearly polarized along the vertical direction. Equivalently, an electromagnetic wave can be polarized along any other direction perpendicular to the direction of propagation. Polarization can be described in terms of its components along the vertical and horizontal directions. For example, diagonal light is a superposition of both horizontal and vertical waves that are in phase. A superposition of horizontal and vertical waves that are out of phase – the peaks of one wave align with the troughs of the other – will give anti-diagonal polarization. These are all types of ***linear polarization***.

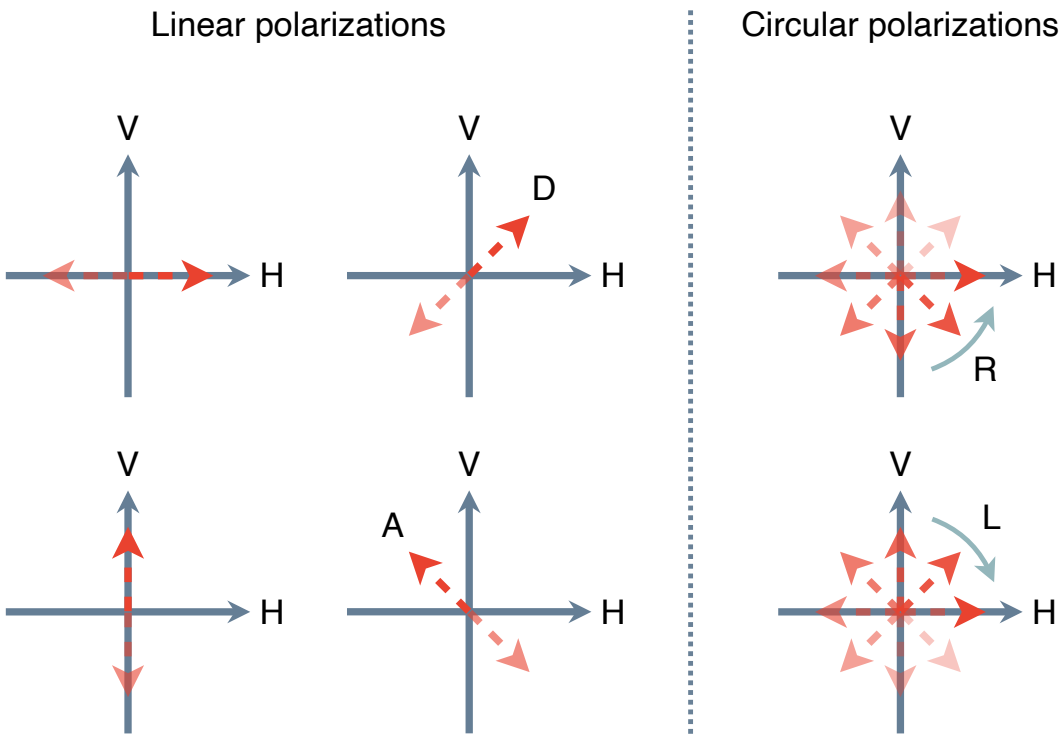


Figure 3.6: Different polarizations of the electric field as seen by an observer when light is propagating out from the paper: vertical (V), horizontal (H), diagonal (D), anti-diagonal (A), right (R), and left (L) circular.

More generally, we can describe elliptical polarization where the electric field precesses around the arrow indicating the direction of propagation. The most common are left and right circular, where the electric field rotates either clockwise or anti-clockwise as the wave propagates. In Figure 3.6, we show both linear and circular polarizations mentioned from the perspective of light propagating out of the page.

Path encoding

We are not limited to polarization to encode information and it may be beneficial to choose another property depending on the specific application. Consider the situation on the left-hand side in Figure 3.7 where a single photon can be transmitted or reflected by a beam splitter, defining two different directions or paths, labeled in the figure as *a* and *b*. We can use these paths as our $|0\rangle$ and $|1\rangle$ states. To encode different superpositions, we can change the splitting ratio of the beam splitter which changes the probability that photon will be found in either path. Path encoding is more commonly used for computation rather than quantum communication. However, we can convert between polarization and path encoding by using an optical component called a polarizing beam splitter that separates the horizontal and vertical polarization components into different paths.

Time-bin encoding

Finally, let us consider encoding information in the arrival time of a photon at a detector. We define two temporal windows, or bins, that we will call early and late time-bins and represent the $|0\rangle$ and $|1\rangle$ states. Our qubit is then encoded in a photon traveling in either the early time-bin or the late time-bin

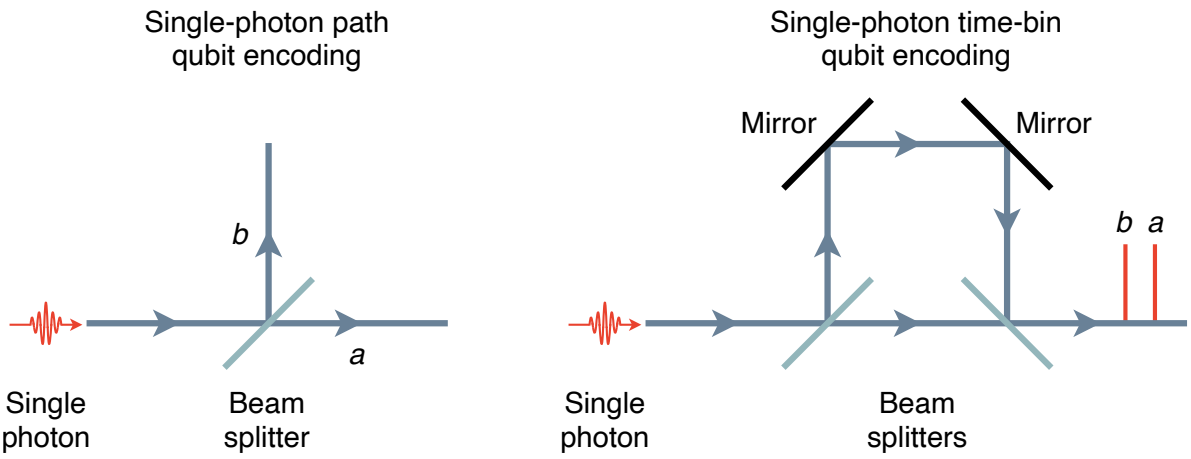


Figure 3.7: Single-photon path and time-bin encoding. The states $|0\rangle$ and $|1\rangle$ are represented by *a* and *b*.

or a superposition of the two, using the apparatus shown on the right-hand side in Figure 3.7. A photon can travel through either the short path or long path between the two beam splitters, encoding early and late time bins, respectively. As with the path encoding, we can vary the probability that a photon is sent through the short or long path allowing us access to any superposition state. In Chapter 5 we will see how errors can be introduced along different types of quantum channels. Time-bin encoding is often used in quantum communication, particularly where optical fiber is used, as both the states travel along the same channel. This can minimize the noise between the $|0\rangle$ and $|1\rangle$ states meaning time-bin encoded qubits are less sensitive to certain errors.

We have introduced how one can encode a qubit using the polarization, path, or arrival time of a single photon. These multiple options make single photons a versatile tool in quantum communication and the only viable solution for achieving long distance communication. In later chapters, we will see how photons will be a fundamental part of quantum communication protocols and networks. The next chapter will introduce different components to create, manipulate, and measure single-photons.

4 Components

So far in this booklet, we have introduced how light can be described with quantum theory and how such properties allow for new information processing and applications. We will now introduce some of the components needed to implement the technology in the real world, forming the building blocks of quantum communication links.

Classical optical communication uses bright pulses of light to encode information, typically generated by lasers. These pulses may contain billions of photons meaning they can tolerate losing some of the photons to the environment. Measurements are made by collectively measuring all the photons using a material that converts the light to an electrical signal. For long distances, the pulses can be repeated by measuring the signal and creating a new, brighter light pulse.

Quantum communication exists at the *single-photon level* and the traditional bright light pulses cannot be used. Instead, new methods of generating individual photons need to be developed. As our information is encoded in a single particle, loss can be fatal. Engineering efficient, low-loss components is necessary especially as we are no longer able to repeat the quantum information in the usual way due to the no-cloning theorem. Measurement devices need to be adapted to extremely low energy levels.

Single-photon sources

Light has proven the most effective medium for transmitting information over large distances. However, to transmit quantum information, we require a system that is quantum mechanical – in this case, *single* photons. Generating single photons is not easy and we have been working on the technology for decades. Currently, there are several options for single-photon generation. Each comes with its own strengths and weaknesses that might make it appropriate for one application but not another. To assess and compare the different approaches, it is important to introduce relevant terminology used to describe the generation performance and to compare this to the *ideal* case.

An ideal single-photon source would generate one, and only one, photon when requested and no photons otherwise. A source that has this property is called *deterministic on-demand*. A device operating in the real-world usually does not behave perfectly, so many on-demand sources have a probability of less than 100 % that a photon is generated when requested. Similarly, it may produce photons at other times when not requested. This is a central challenge in quantum communication.

Photons have many properties, such as wavelength or polarization, that we must be able to control precisely for our applications. The *fidelity* of photon creation is a measure of how close the new photon is to the intended state. In the ideal case, every photon produced from a photon source would be in exactly the intended state. Two photons that are identical, i.e., that are the same in every measurable way, are referred to as *indistinguishable*.

One characteristic that will impact the fidelity is the time at which the photon is produced. There will be some uncertainty between the time at which a photon is requested vs its production. This

uncertainty is known as *timing jitter* and is something we aim to minimize. Jitter will also impact the *repetition rate*, which is how many photons can be produced each second.

The ideal wavelength of photons used is dependent on the application. For example, modern telecommunications networks typically use infrared wavelengths to minimize absorption in glass while satellite links will use visible wavelengths to minimize loss through the atmosphere.

Finally, each technology will have strict bounds on operating conditions such as the temperature and pressure. Many quantum technologies require ultra-high vacuum and cryogenic systems (ultra-low temperatures) to reduce noise. Such systems are impractical in many scenarios, for example in satellites where power and cooling capabilities are limited.

To discuss the different approaches to developing single-photon sources, we will broadly separate the technologies into three categories – probabilistic, deterministic, and quasi.

Probabilistic

Even though deterministic photon sources are the goal, probabilistic sources have proven useful in applications such as quantum metrology and are still a useful resource for quantum links.

Instead of producing a single photon, a probabilistic source produces a correlated pair of photons at random. As we have two photons, we can measure the presence of one to provide a signal which *heralds* the presence of the other. The unmeasured photon can then be used in our application.

Probabilistic sources were the first technology developed to generate single photons. Initially, these sources used an atomic cascade to probabilistically create a correlated pair of photons. In the early 1980s, Alain Aspect famously used calcium atoms to generate photons entangled in polarization, and used them to experimentally verify that quantum mechanics does not have an underlying classical explanation[7]. Many other atomic systems have been used as photon sources but have since fallen out of use.

Today, the two main approaches to probabilistic single-photon sources are spontaneous parametric down-conversion (SPDC) and spontaneous four-wave mixing (SFWM). Both processes depend on specific properties of a material, meaning that it must be carefully selected. A bright laser illuminates a nonlinear material and either one photon in the case of SPDC or two in the case for SFWM from the laser are converted into two output photons. The output photons are constrained by conservation of momentum and energy, ultimately leading to pairs of photons which are correlated in some of their properties.

There are many crystals that have been discovered that can be used as probabilistic photon sources. Some commonly used materials include beta barium borate (BBO) and potassium dihydrogen phosphate (KDP) for SPDC, and silicon for SFWM.

While the probabilistic nature of these photon sources limits their uses, they do have some benefits over other sources. Different materials allow photons to be produced at different wavelengths making them very suitable for a wide range of applications. The process does not require cryogenic temperatures or ultra-high vacuum, making them relatively simple. However, as the process is probabilistic, it is possible that multiple photon pairs are generated at the same time. To minimize this

possibility, the generation of photon pairs is kept low which limits the scaling capability for quantum technologies that require rapid photon-pair generation.

Finally, there is a proposal that extends the idea of heralding to include many probabilistic sources operating simultaneously. This idea is called multiplexing. By having many sources generate pairs of photons at the same time, we can use a herald signal to quickly switch the correct source to the output. As part of the SCaN program, NASA is developing multiplexed and highly efficient photon sources[8].

Deterministic

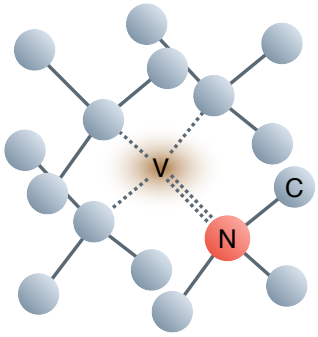
To understand a deterministic single-photon source, consider the energy levels of an atomic system. When an electron decays from a high energy level to a lower energy level, a photon is emitted, as was discussed in the previous chapter. The energy of the photon is given by the difference in energy between the two atomic energy levels. As this process yields only one photon, these systems are known as *single emitters*. The challenge is controlling the decay process so that photons can be produced on-demand.

To guarantee that only one photon is produced, the atomic system needs to be isolated. For atoms, a common method is to use a magneto-optical trap (MOT) to capture and cool an atom that is then dropped through an optical cavity which stimulates a photon to be emitted. These systems to isolate atoms are complex, limiting their use to lab environments. The next evolution was to move from atoms to ions; an electron is removed from an atom giving it a positive charge. This allows individual ions to be held in place by an externally applied electromagnetic field for days or months. Current ion-trapping devices often use microfabricated surface traps, which are much like computer chips, making them easily scalable.

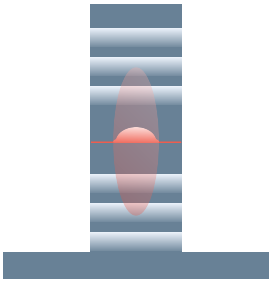
When a photon is produced from an atom or ion it is emitted in a random direction. This means a system needs to be carefully designed to capture the photons while still allowing the necessary control.

To avoid building the complex systems required to isolate and trap individual atoms, researchers have sought to replicate them in solid-state systems which exhibit atom-like properties[9]. It is for this reason that these systems are commonly called artificial atoms. Solid-state systems avoid the need for complicated trapping devices and are a leading technology for real-world applications.

A leading solid-state single-photon source is called a *quantum dot*, where a carefully engineered semiconductor structure confines individual excitons – a quasi-particle made from an electron-hole pair. A single photon can be produced deterministically by applying either a laser or electrical pulse which excites the exciton to a higher energy level. Figure 4.1 shows a quantum dot placed in a microcavity, where the optical cavity is used to enhance the efficiency of photon generation and provide a well-defined direction of photon emission. Quantum dot sources typically operate at cryogenic temperatures to achieve the best performance, which can limit their applicability and scalability. The wavelength of photons depends on the atoms used to create the quantum dot with systems developed for UV, visible, and near-infrared operation.



Nitrogen-vacancy color center in a diamond lattice



Single quantum dot in a microcavity

Figure 4.1: Color center and quantum dot single-photon sources.

Other popular single emitters include isolated defects in nanocrystals that are usually called color centers due to their fluorescence when an external laser is applied. Color centers are formed when an atom in a crystal is substituted with a different atom leaving a vacancy in the lattice. One such color center is shown in Figure 4.1. In certain cases, an electron in the vacancy forms a three-level system that can be used to generate single-photons by irradiating it with an external laser. The most studied color centers are formed when a carbon atom in diamond is replaced with either a nitrogen or silicon atom. These defects can occur naturally but are usually created artificially through ion implantation. Attempts to increase photon collection efficiency include adding micro-lenses over the nanocrystal to focus the photons. The wavelength is not easily tunable and is usually in the visible spectrum. While color centers can operate at room temperature, cryogenic temperatures are preferred to minimize thermal noise which can reduce fidelity.

Quasi

Light is quantum, meaning that even the lasers that we used for modern communication can be described in terms of photons. A bright laser pulse contains too many photons to exhibit quantum effects. However, by attenuating the laser to very low power we can recover quantum phenomena. The state produced is not exactly a single photon and we must instead describe the state as a probabilistic mixture – a superposition of many possible numbers of photons. The state will have a probability of zero photons, another probability of one photon, some probability of two photons, and so on, that will depend on the brightness. This state is different from the probabilistic sources above as we are unable to herald.

While these sources are far from ideal, they utilize existing and well-developed hardware making them accessible. As such, quasi-single-photon sources have been instrumental in developing quantum links in the interim period before other single-photon sources mature. They have also been used extensively in quantum key distribution.

Entanglement generation

Entanglement is an essential resource in the development of quantum networks, so it is important to understand how we generate entangled states using real world devices. Processes such as SPDC

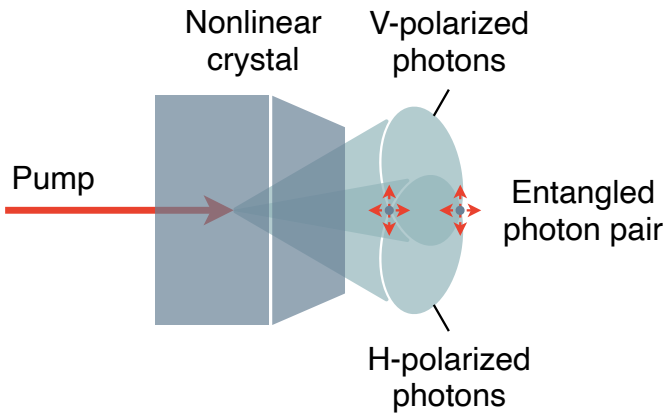


Figure 4.2: Source of polarization-entangled photon pairs based on SPDC.

and SFWM are not only suitable for the probabilistic generation of single photons but can also be used to generate entangled photons.

We previously described how SPDC, for example, is used to produce pairs of photons, wherein one photon from a pump spontaneously converts into two photons in a process conserving energy and momentum. If we consider the polarization of the photons that are generated, we see that due to conservation, the generated photon pairs follow trajectories constrained along the sides of two cones, as shown in Figure 4.2. The axes of the cones are symmetrical according to the trajectory of the pump photon and correspond to different polarizations. The vertically polarized photons follow a cone upwards, while the horizontal photons travel downwards.

The process of SFWM can also be used to generate polarization-entangled photons but takes in two pump photons to generate an entangled pair. SFWM can be performed in optical fiber, which is beneficial for fiber-based quantum communication. More broadly, these processes can be used to create entanglement using properties of light other than polarization such as wavelength, path, or timing.

Interestingly, particles do not need to be the same to be entangled, and recent advances in hybrid quantum technologies rely on entangled pairs of different particles. This will be of particular importance in the design of quantum networks connecting many different quantum devices, such as quantum computers which are built using different quantum systems. Many of the deterministic single-photon sources introduced above are also being developed for this purpose. For example, an electron and photon can be entangled by exciting quantum dots with laser pulses[10]. In Chapter 8, we will see how these devices will be used in a quantum network. However, developing practical methods of entangling hybrid particles such as these remains a challenge.

Single-photon detectors

Generating single photons is only one part of a quantum communication link. We also need a method of measuring when a photon has arrived. This is the role of single-photon detectors which convert the energy of a single photon into an electrical signal that we can easily measure.

An ideal single-photon detector would report a measurement every time a photon arrives. This property is referred to as the *efficiency* of the detector which, in the ideal case, is 100 %. We would also expect that no measurements would be reported if a photon was not present. These events are known as *dark counts* and would have a zero probability of occurring in the ideal case. In a real detector, environmental factors will cause false-positive events where the detector reports a photon when none arrived.

The timing of the measurement will be important. In real devices, there is an uncertainty in the time between when a photon arrives and the detector reporting a measurement. This is known as a *timing jitter* and should be minimized. Similarly, detectors often require time to reset after a successful measurement and will be unable to detect photons until fully reset; a property known as *dead time*. Both the timing jitter and dead time will impact how quickly a detector can register different photon events; to ensure a high detection rate, both need to be small.

Until now, we have only considered a detector measuring a single photon. However, it is natural to consider the case when multiple photons arrive simultaneously. Most commonly, single-photon detectors can only report if a photon was measured or not and give no information about the number of photons. These are referred to as *threshold* detectors and the measurement outcome will look the same for one photon as for multiple photons. Some single-photon detectors are *photon-number resolving* meaning they are capable of also reporting the number of photons that arrive.

Finally, it will be important to consider the operating conditions of the detector. Single-photon detectors will often require cooling, which may be to cryogenic temperatures, or need to be operated in ultra-high vacuum. This will place constraints on where they can be operated and, in some cases, prohibit operation on a satellite.

This section will introduce some of the most prominent devices that are used for single-photon detection. Using the typical characteristics above, we will be able to compare the different technologies and the suitability for quantum communication applications.

Photomultiplier tube

The longest-used single-photon detector is the photomultiplier tube (PMT), which uses the photoelectric effect that was instrumental in the initial discovery of photons. The process is shown in Figure 4.3 and starts with a photocathode – a material that when hit by a photon emits an electron. The electron is accelerated towards a series of electrodes, called dynodes, which are housed in a vacuum and biased in the kilovolt range. The initial electron causes more electrons to be emitted which amplifies the signal. By the end of the amplification, the signal contains more than one million electrons which can be easily measured by standard electronic equipment.

While the technology is old, PMTs are still commonly used to measure photons with UV or visible wavelength and can be 40 % efficient. They operate at room temperature and offer low noise (roughly a few dark counts per second), fast response, and low timing jitter. The photocathode can be large making PMTs suitable for light that is not perfectly aligned. However, operation requires very large electrical bias, and the lifetime of the device can be limited due to the requirement for a vacuum chamber.

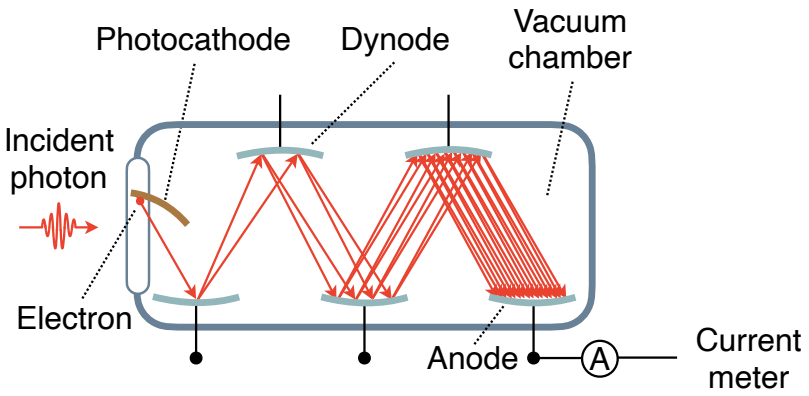


Figure 4.3: A photomultiplier tube (PMT) in which an incident photon results in an electron cascade between dynodes, amplifying the signal, and allowing for single-photon detection.

The dynodes can be replaced by a single plate with microchannels to amplify the signal making the device more compact. NASA Goddard Space Flight Center (GSFC) is evaluating microchannel plate PMT (MCP-PMT) detectors that are suitable for space flight.

Single-photon avalanche diode

In the pursuit of developing a more robust single-photon detector, a similar process was developed that replaced the vacuum chamber with a semiconductor crystal. The electrodes are replaced by a diode – an electrical component that allows current to pass in only one direction. Modern diodes are made from two layers: one is positively charged while the other is negatively charged. A photodiode is a diode that exhibits the photoelectric effect. When we shine light on a photodiode, we can eject electrons and create a current in the forward direction of the diode. Measuring this current allows us to measure how much light was illuminating the diode. However, the current caused by a single photon is too small to measure so we must amplify the signal.

Avalanche photodiodes (APDs) are created when a reverse voltage is applied to a photodiode. When light hits the material, it causes electrons to be ejected. As we have applied a reverse voltage, an ejected electron is accelerated towards the positive terminal. This causes other electrons to be ejected, which then eject more electrons. This amplifies the current to one we can measure.

In the case of a single-photon avalanche diode (SPAD), the electrical voltage applied is more than the diode breakdown voltage; this is the voltage that will cause current to run in reverse across a diode. A photon causes a single electron to be ejected which causes an avalanche of electrons as before. However, as the voltage is greater than the breakdown limit it creates a self-sustaining current which we can measure. As with PMTs, we have amplified a single electron to a signal at a level we can measure.

SPADs have become a common alternative to PMTs in quantum communication due to their robustness and higher detection efficiencies. The semiconductor diode can be made from different materials that are suitable for different wavelengths. For example, silicon is an effective material for visible light with up to 85 % efficiency but is transparent for infrared light. Instead, indium gallium arsenide (InGaAs) diodes are used for telecommunication where detection efficiency is limited to

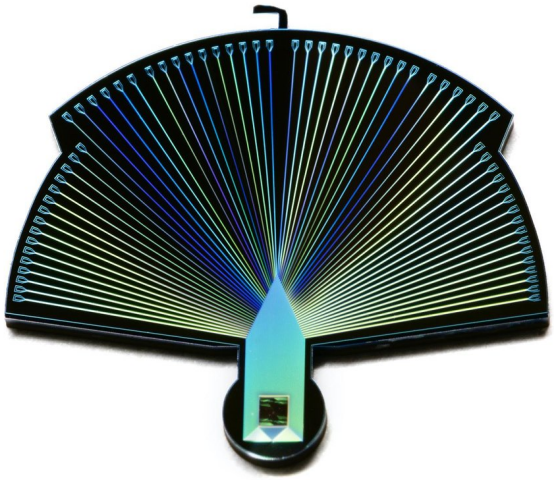


Figure 4.4: Performance-Enhanced Array for Counting Optical Quanta (PEACOQ) superconducting detector developed by NASA JPL. Smaller than a dime and made up of 32 niobium nitride superconducting nanowires on a silicon chip, these detectors could help form a global quantum communications network. **Image Credit**: NASA/JPL-Caltech[12].

around 20 %. The avalanche effect takes less than a nanosecond, meaning SPADs can be operated very quickly, and they can be operated at room temperature. The dark count and timing jitter is typically higher than the best performing PMTs, however, cosmic radiation has been shown to substantially increase dark count noise[11].

Superconducting detectors

To increase the performance of single-photon detectors, a new approach has emerged in the past few decades that leverages superconductivity. Normal electrical wires have a resistance which decreases as the temperature is reduced. A superconducting material will, below a specific critical temperature, have zero resistance. This property can be used to detect single photons.

At the heart of a superconducting detector is a wire that is cooled to below its critical temperature. An electrical current is passed through the wire which keeps the wire just below the critical point at which it will no longer be superconducting. When a photon hits the wire, it causes a local hotspot where the metal is no longer below the critical temperature and, therefore, no longer superconducting. Consequently, this creates a voltage signal that is amplified and measured.

Superconducting detectors represent the state-of-the-art in single-photon detection with efficiency above 98 %, low timing jitter, and low noise. However, this comes at a cost of practicality. Superconductivity has only been demonstrated in materials in extreme environments. Typically, a superconducting detector requires temperatures below 4 kelvin and an ultra-high vacuum. Reaching these conditions is demanding and power intensive which would preclude their use in satellites. However, they are suitable for operation in ground-stations particularly when they can be shared between many satellites in a satellite-ground configuration.

The superconducting material and design of the system can be adapted for different wavelengths or requirements - for example, to favor lower dark counts over higher efficiency. Typically, a thin wire is used in a meander to fill a larger space. These are referred to as superconducting nanowire single-photon detectors (SNSPDs). An optical cavity is created around the nanowire to enhance the interaction with incoming photons.

Photon number resolution is possible with superconducting detectors as more photons will cause a larger heating effect. The most common variety of such detectors are transition edge sensors, although SNSPDs have been shown to exhibit the same effect.

NASA Jet Propulsion Laboratory (JPL) is developing SNSPD arrays like that shown in Figure 4.4, capable of high-rate detection for quantum communication for optical ground stations[12]. These detectors will form part of optical ground stations for NASA's Deep Space Optical Communication (DSOC) project.

Supporting equipment

For quantum communication applications, it will not be sufficient to generate and measure photons alone. We will also need components to encode information in the light, synchronize nodes, and control the equipment. Supporting systems will be needed to achieve cryogenic temperature and ultra-high vacuum and we must consider how quantum links can coexist with modern classical communication networks.

As we saw in Chapter 3, there are many properties that can be used to encode quantum information in light. Different components will be needed depending on the property chosen. For example, polarization is commonly used for free-space quantum communication. Rotating the polarization can be performed using transparent materials that have a different refractive index depending on the polarization of light – a property known as birefringence. By rotating the material in the path of the light, we can cause the polarization to rotate. We can even use these materials to separate the two polarizations. Alternatively, we can use material where the refractive index changes depending on an applied electric field, such as a Pockels cell.

Many of the single-photon sources and detectors above require cryogenic temperatures to operate. To achieve such low temperatures, either helium or nitrogen is cooled to its liquid state and then pumped to the device. The liquid will then boil off and can be collected and recycled back to be cooled. The device being cooled is contained in an ultra-high vacuum chamber to isolate it from the environment.

Finally, it is likely that quantum communication will leverage existing communication networks so there is a need for quantum and classical communication to coexist. One method, which is common in classical communication, is to combine multiple signals of different wavelengths into a single channel. This is known as wavelength-division multiplexing and is typically used to increase the capacity of a channel. We can employ the same technique to allow quantum and classical information to exist on the same channel by having them at different wavelengths.

We have seen how cutting-edge components allow us to generate, manipulate, and detect quantum signals. How can we use this technology to *communicate* quantum information between distant parties? In the next chapter we explore the means of connecting different parties who each have access to these components, by way of quantum channels, or links, that run alongside classical channels for communication. Quantum links are another essential building block in future quantum communications systems and networks.

5 Quantum Links

There are many technological advances required to reach a fully-connected quantum network that is on par with the classical networks today. Currently, quantum communication is limited to what we will refer to as ***quantum links***. These are channels for sending and receiving quantum information which connect "mostly classical" nodes. At nodes, many of the components discussed in the previous chapter are used to send and receive quantum signals, with processing of information performed classically. In future, quantum links may connect networks of quantum processors, but for now channels have few capabilities beyond sending quantum information between two, pre-determined, classical nodes.

The quality of a link is determined by the amount of quantum information that can be transmitted without degradation or loss. Thus, no matter the type of link used, be it an optical fiber or free space link, the main challenge is channel error.

This chapter will introduce the different aspects of quantum links; what considerations need to be made when transmitting quantum information and what different types of system are available to us for connecting people and places around the globe - including efforts outside of our atmosphere.

Channel errors

In any real-world system, errors are inevitable and come in many forms. When considering communication, transmission loss is one of the biggest limitations. When we send a signal, how sure are we that it will arrive? Loss depends heavily on the type of channel chosen to connect parties, as well as the system that is used for encoding the information. For example, the wavelength of light will affect loss.

We characterize loss of a channel with a metric known as ***attenuation*** which is a logarithmic scale similar to what we use to measure audio volume or earthquake magnitude. It is given in units of decibel (dB) and can be thought of as the proportion of signal *lost* during a transmission.

In classical communication, transmission loss does not significantly limit distance since repeaters can be used to detect, amplify, and re-transmit optical signals, compensating for any losses incurred. For quantum communication however, the no-cloning theorem and the fact that measurement of individual photons disturbs their quantum information, renders classical repeater technology ineffective. Furthermore, as we use single photons to encode quantum information, if a photon is lost then that information is entirely lost with no means of recovery. Hence, sending quantum information over arbitrarily large quantum links is not possible and remains one of the biggest challenges in scaling current networks.

Beyond loss, other errors can also limit communication. In classical communication, this is limited to bit-flip errors. We may have transmitted a 0 but by the time it arrives it has been flipped to a 1. Errors in quantum communication are more complex owing to the possibility for a qubit to be in a superposition state. Quantum information encoded in a single photon is far more sensitive to noise

and fluctuations in a channel than classical information encoded in bright laser pulses. For this reason, we refer to channel errors as ***decoherence*** to encompass these new forms of error.

Attenuation and decoherence are critical features to consider for quantum links, which rely on the principles of quantum mechanics for information transfer and processing. High-quality links are essential because photon loss and state decoherence can significantly degrade signal quality, achievable distances, and ultimately limit the feasibility of quantum communication systems.

Fiber links

In the range of long-distance quantum communication, optical fibers provide a convenient means of signal transmission that is free from atmospheric effects. Optical fibers comprise a core into which light is injected, surrounded by a transparent cladding material with a lower refractive index. Light is confined in the core due to a phenomenon called *total internal reflection*, allowing the optical fiber to guide light through bends and twists from one end of fiber to the other.

Today, optical fibers are used ubiquitously across computing, space applications, defense, and sensing. The current fiber-optic framework used for global connectivity provides a convenient platform for develop quantum communication capabilities. Large-scale, fully-quantum networks have yet to be realized, since novel fiber-optic infrastructure may be necessary. But in the meantime, hybrid classical-quantum networks have taken advantage of the fiber-optic networks already in place[13–15].

Signal errors in optical fiber

Correct functioning of any communication link relies on enough signal reaching the receiver without being lost or degraded. Attenuation is the reduction in power of an optical signal as it is transmitted, and is caused by passive components like fibers and connectors. Errors can also be caused by other effects such as dispersion or polarization rotation. Dispersion is an optical effect where different wavelengths of light move at different speeds through a material. In optical fiber, this can cause a signal to spread out over large distances. Optical fiber can also cause the polarization of light to rotate which can introduce errors.

Attenuation in an optical fiber can be separated into two categories: intrinsic loss, due to absorption and scattering incurred by the material itself, and induced fiber loss resulting from manufacturing error. Although, unlike free-space links, optical fibers hold up very well against external atmospheric effects, optical fibers can expand and contract due to small changes in ambient conditions, resulting in decoherence of the fragile information encoded in the photons.

We can calculate the attenuation of a channel, often labeled η, by comparing the intensity of a signal before and after a communication channel. The equation is

$$\eta = 10 \times \log_{10}\left(\frac{\text{Output intensity}}{\text{Input intensity}}\right).$$

If instead we wish to consider a single photon through a channel, we replace the intensity with the probability that the photon is not lost through the channel. This yields the equation

$$\eta = 10 \times \log_{10} (\text{Probability photon not lost}) .$$

For example, if a photon has a 50 % probability of not being lost over a channel, we would say that the channel has approximately 3 dB attenuation.

In practice, photon losses in optical fibers result in transmission decaying *exponentially* with distance. A typical telecommunication fiber has an attenuation of 0.2 dB per km which means for 1 km of fiber the transmission probability of a photon is 95 %. However, by 500 km that probability is instead 10^{-10}. This means that if we were to send 10 billion photons per second over 500 km, we would only expect one to arrive at the other end each second. For an even longer link of 1000 km, the increased attenuation would mean one photon reaching the receiver every 300 years!

Ultra-low-loss fiber

Reduction in fiber loss accelerated quickly after their development for telecommunications. By 1979, fiber attenuation had reached 0.2 dB per km for 1.5 µm light[16], which is the typical value for today's standard fibers with germanium-doped cores. In 1986, fiber loss of 0.154 dB per km was reported using a pure silica core[17]. Reaching below 0.15 dB per km is a difficult task as we now approach the fundamental limit for optical fiber. However, research efforts have continually improved manufacturing procedures, and today the lowest attenuation achieved in a lab is 0.14 dB per km[18].

Because of its wide bandwidth, ZBLAN and other exotic glasses are interesting prospects to produce optical fiber. However, the influence of gravity on the manufacture of these glasses results in unwanted crystallization, in turn leading to increased scattering losses in the fiber. Because of this, Dr. Dennis Tucker of the Marshall Space Flight Center suggested that the fabrication of ZBLAN in microgravity might prevent unwanted crystallization[19]. A small experiment was flown for the first time on NASA's KC-135 reduced gravity aircraft[20], and subsequent experiments took place on parabolic flights in microgravity.

In 2014, a technical review meeting was held at NASA Ames Research Center, bringing together experts in both microgravity and terrestrial exotic optical fiber manufacture. Shortly after, NASA awarded two grants to Physical Optics Corporation (POC) and Fiber Optics Manufacturing in Space (FOMS, Inc.)[21] for using the microgravity environment to improve the quality of ZBLAN.

Free-space links

Free-space, or atmospheric, channels refer to the absence of fiber optic cables that enable most terrestrial communications. Instead, light is sent between sender and receiver directly through the atmosphere, along line-of-sight. The most important reason driving the development of free-space quantum communication links is the potential to overcome fundamental limitations restricting the scalability of fiber links. Free-space links have the potential to significantly reduce loss at long distances due to the attenuation being fundamentally quadratic with distance, as opposed to exponential for equivalent optical fiber links. As such, free-space channels allow for long-distance

communications, such as intercontinental links, where physical fiber connections can be limited in scope.

Free-space channels, however, have their own unique challenges as well. Atmospheric turbulence causes errors due to processes like scattering as the signal is transmitted through the atmosphere. Also, diffraction and solar noise can further decrease the signal-to-noise ratio resulting in increased communication errors. Current efforts in space-based quantum communication can be found at the Air Force Research Laboratory (AFRL) and NASA. Technologies such as adaptive optics are successfully being used to mitigate sky noise effects (turbulence, solar background, etc.) on atmospheric channels enabling further progress with the quantum communications protocol in space[22].

Satellite quantum links

In the case of satellite communication, beam diffraction, rather than absorption, is the dominant cause of loss, meaning channel loss scales *quadratically* with distance. For example, a satellite linking two ground stations 1200 km apart is 15 orders of magnitude more efficient in terms of loss than a fiber link[23]. Also, most satellites are fast-moving objects able to physically travel between distant locations over the globe and allow line-of-sight connections far beyond what is possible using terrestrial links. This may allow a drastic reduction in the complexity of quantum networks, that would otherwise comprise many ground stations and relays. In fact, entire chains of nodes may be replaced with a single satellite circling the globe and servicing many ground stations.

Although satellite links suffer negative effects caused by the weather, most of these issues arise in the troposphere – the lowest atmospheric layer at around 20 km. As an example, for a free-space optical link between ground station and a satellite in low-Earth orbit, the path of the photons is virtually in a vacuum, apart from the lower 10 km of atmosphere. This means, for most of the journey, photons experience negligible absorption and scattering.

Challenges

Transmitting light between a satellite and Earth has unique challenges. For example, the telescopes on both the satellite and the ground stations require tracking so that they remain pointed to one another to optimize transmission. Weather and atmospheric conditions can complicate this pointing; eddies and particles in haze or fog generate random fluctuations in the relative permittivity of the air. This in turn causes random deflection and distortion of the light beams sent through the atmosphere. Finally, geometrical losses due to a finite collection aperture, and random modifications of the phase front, lead to reduced transmittance overall.

The threat of signal jamming is of particular importance to secure satellite quantum communications but is relevant to other forms of free-space communication. Optical jamming of signals can be achieved both from line-of-sight targeting of detection devices, or in the case of satellite-ground communication, form outside line-of-sight by reflecting light off the transmitting satellite. Unfortunately, this attack can be effective even 1000 km away from the ground station[24], presenting a major challenge in the deployment of satellite quantum key distribution.

Payload

Realization of satellite-aided quantum communications requires both ground-based and space-based segments. The space segment is composed of one or more satellites fitted with a payload, including a source of photons and detectors, depending on the application. For example, a satellite may be used as a mid-point source between two ground stations, preparing and transmitting entangled photons between them to create an entangled link (each ground station has one photon from an entangled pair). Also in a payload may be an optical terminal and processor, often with a means of onboard measurement of transmitted quantum state fidelity. Other apparatus onboard monitors the optical, thermal, and mechanical status of quantum devices. The satellite must also have devices for classical communication and processing, for transmitting radio frequency signals to receivers for related protocol data exchanges, for example. In downlink scenarios, an onboard optical terminal includes telescopes used for directing photons towards ground stations, which are mounted on remote controlled actuators for pointing, acquisition, and tracking (PAT). Any space-based segment must be as lightweight as possible, so minimizing both the number of devices and their weight is a major consideration for satellite-based communications.

Pointing, acquisition, and tracking (PAT)

Line-of-sight must be maintained between ground stations and moving satellites, or for inter-satellite communications, therefore PAT technology is an important feature of satellite links. It allows for accurate transmission of an optical signal to the receiving aperture using precise tracking. This mostly compensates for the error caused by the fast relative motion of the station and satellite. Tracking is usually aided by beacon lasers, and a laser master clock for ground-satellite synchronization, ensuring the PAT devices remain calibrated.

Implementation of ***adaptive optics (AO)*** in satellite links can help with tracking errors and misalignment and helps decrease losses caused by beam distortions. AO are made up of deformable mirrors or lenses that correct wavefront errors in a propagating beam[25]. They can be used in a pre-correction approach wherein the channel is first characterized for the effects of turbulence on the signal and phase corrections are made accordingly before the signal is sent. This is most useful in ground-satellite architectures both due to the bulky nature of AO components but also the fact that, as will be discussed later in the chapter, signal distortions due to atmospheric effects are more pronounced in ground-satellite links.

To minimize losses due to the atmospheric channel in ground-satellite communications, quantum space and ground terminals employed by NASA will use adaptive beam control via a fast-steering mirror to compensate beam tilt[26] and AO at the ground terminal to compensate higher-order turbulence-induced aberrations[27]. In satellite-ground links, PAT technology must be an integral part of design, and for this much research has been carried out by MIT Lincoln Laboratory and NASA JPL, both labs leveraging experience in AO and PAT technologies used for the development of quantum links[4].

Satellite link architecture

To support large-scale continental links without the use of repeaters, quantum communication satellites and other spacecraft require simultaneous line-of-sight to ground stations. The ground stations may then themselves be connected by fiber, and act as nodes in a local fiber-based terrestrial quantum network such as that in development under the SCaN program's Quantum Entanglement Distribution in Space Optical Network (qEDISON) mission concept[4]. This seven-year proposal aims not only to establish satellite-aided links between ground stations within the US, up to 1200 km apart, but also between the US and other continents (on the order of 6000 km).

Ground stations

Much like satellites, ground stations in a quantum network can house components for photon generation, manipulation, detection, and PAT to keep line-of-sight with satellites. Unlike satellites, they are not limited by the same restrictions in terms of weight and power. However, an important consideration for ground stations is geographic location. Atmospheric conditions such as fog and cloud not only reduce visibility and cause potential link issues, but also differ depending on their latitude and altitude: fog at sea is not the same as fog inland, fog near the poles is not the same as fog at mid-latitude. Finding locations for ground stations which minimize atmospheric effects is important.

Types of satellite orbit

There are several different altitudes at which satellites can orbit the Earth, some of which are shown in Figure 5.1, forming links with ground stations and terrestrial networks. Each is relevant to different applications and with its own challenges[28]:

- Low-Earth orbit (LEO) region: the region of space up to an altitude of 2000 km (equivalent circular orbital period of approximately 127 minutes)
- Medium-Earth orbit (MEO) region: the region of space from 2000 km to 35 586 km
- Geosynchronous orbit (GEO) region: the region of space from 35 586 km to 35 986 km (GEO ±200 km).

Thousands of low-Earth orbit (LEO) satellites are in operation today, primarily addressing science, imaging, and low-bandwidth telecommunications needs. Medium-Earth orbit (MEO) satellites have historically been used for Global Positioning System (GPS) amongst other navigation applications but are more generally useful for reaching remote areas where laying optical fiber is not viable. LEO satellite provides better signal strength, least signal propagation delay since it is closest to earth, creating good links between cities, while satellites in higher MEO orbits would allow intercontinental quantum communication and allow the creation of a global, all-day quantum communication network.

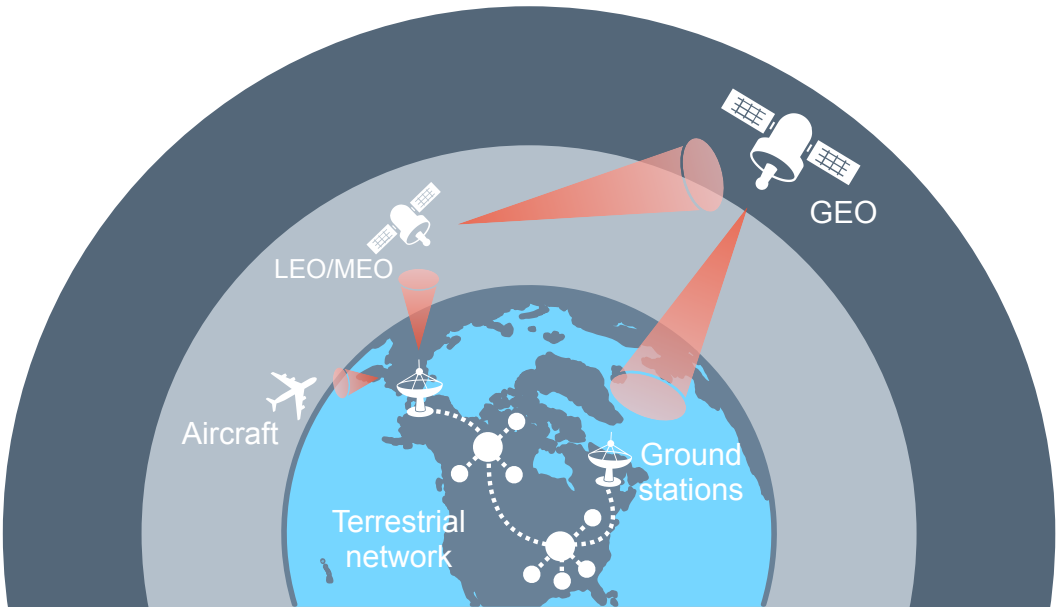


Figure 5.1: Concept of aerial and satellite quantum communication network.

Uplink vs. downlink

In uplink, the signal is transmitted from the ground station to the satellite, whereas in downlink the satellite is the transmitter while the ground station is the receiver. In both configurations, free-space diffraction and atmospheric extinction has the same effect on the transmitted signal. The fading caused by turbulence however is more pronounced in an uplink scenario, where the beam must first make it through the lower atmosphere. Similarly, thermal noise produced by background sources has different effects; day-time uplink is particularly challenging, whereas for downlink the limitations are less severe[29].

Launching satellites in the real-world

Since 1958, NASA has used radio wave technology for space-based communication. NASA's GSFC Laser Communications Relay Demonstration (LCRD)[30] launched in 2021 aims to demonstrate the benefits of optical communications. Lasers will enable better data rates and allow communications systems to become smaller, lighter, and more efficient. As NASA's first long duration test of optical communications technology, the LCRD mission aims to perfect space and ground station technologies for future optical communications with space.

NASA's SCaN program has several ongoing projects to develop satellite quantum links. These include 5- and 10-year plans towards the development of a user facility - a quantum testbed involving multiple ground stations along with satellites in LEO and MEO orbits and optical communications links. Through near-Earth and deep space networks, SCaN provides NASA science and exploration missions with a full suite of RF communications and navigation capabilities.

The near-Earth network (NEN) will support satellites in LEO up to lunar missions, and a constellation of geosynchronous satellites may be used for tracking and data relay, whereas a deep-space network could provide continuous coverage via three ground stations and radio telescopes.

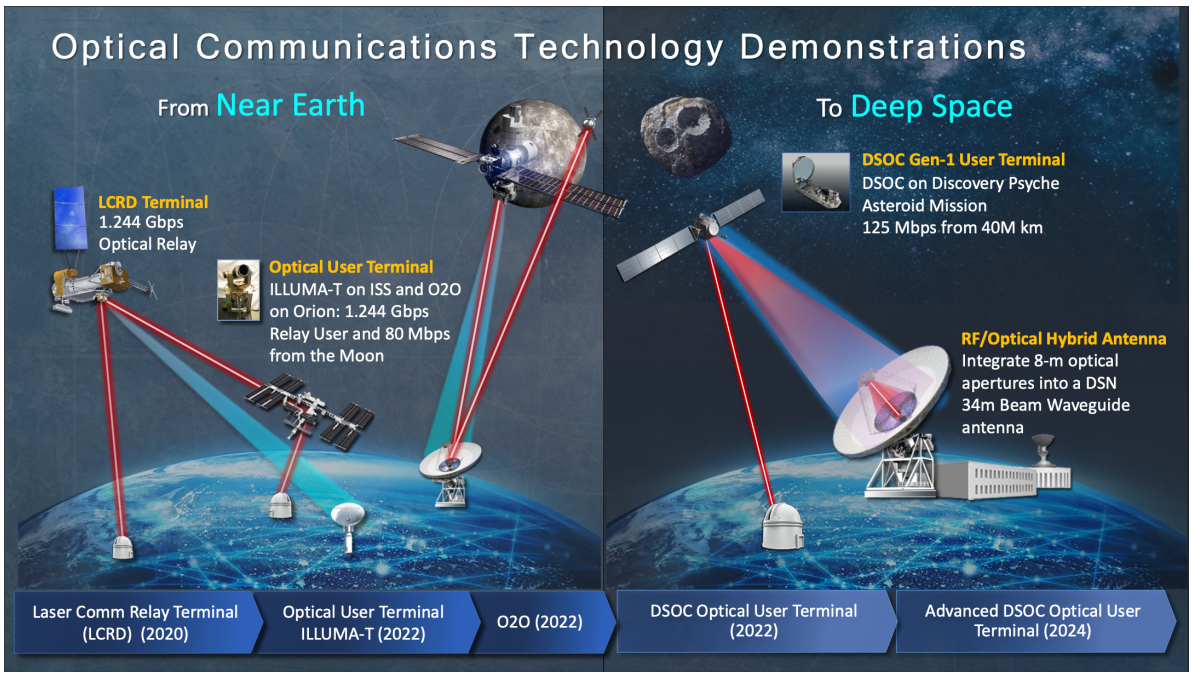


Figure 5.2: A projected timeline of NASA's deep space optical communication activities.

The Deep Space Quantum Link (DSQL)[31] is a mission concept by NASA JPL that seeks to explore relativistic effects on quantum systems. Specifically, DSQL will look at where the effects of relativity affect the outcome of quantum experiments involving teleportation and entanglement distribution, which we will discuss in more detail in Chapter 8. These effects are more pronounced over large differences between gravitational potentials, for example over channels between exotic satellite orbits such as retrograde and highly elliptical. To probe this, a potential orbital deployment for DSQL is a space station orbiting the moon called the Lunar Gateway[32], which will establish a quantum link with a ground station on Earth, or high-altitude UAV platforms orbiting Earth. A timeline for some of NASA's near-Earth and Deep Space projects is featured in Figure 5.2.

NASA's qEDISON proposal is a 7-year, 3-phase project concept to enable space-based distributed and linkable quantum entanglement to one or more ground stations. This huge undertaking would implement the use of entangled photon sources, advanced detector systems, and telescopes on both LEO and MEO spacecraft, with large-aperture optical receivers on the ground, laying the foundations for global quantum communications. The qEDISON proposal will be discussed within the context of quantum networks in Chapter 8. In the next two chapters, we look at some of the applications that are already feasible with the quantum links of today – quantum-enhanced security and quantum metrology.

6 Quantum-Enhanced Security

In our introduction to quantum communication, we have established the means to send and receive quantum information between distant parties. We have seen how we can encode information in photons of light and distribute this information over vast distances with the help of satellites and advanced optical components. In this chapter, we will now explore one of the first applications made possible by such technology – quantum-enhanced security.

Covering the security aspect of communications gives us the opportunity to discuss three important subjects. The first and most obvious is that quantum communication can enable enhanced security, for example in the secret transmission of sensitive data. Secondly, as we will see, certain security applications, in particular ***quantum key distribution (QKD)***, can be implemented today and represent a natural test for the components and technology necessary for quantum communication on a large scale. As such, they are an ideal intermediary step towards more complex quantum communication links and networks. Third, it gives us the opportunity to discuss the impact that other quantum technologies have on the field of communication and security. One particularly important aspect is the threat that quantum computing represents to the security of communication and how the risk can be mitigated. Because of these three reasons, quantum-enhanced security is a natural starting point for our journey into the applications of quantum communication.

Quantum cryptography

Cryptography is the practice and study of methods to secure information in the presence of an adversary, such as an eavesdropper in communication protocols. As many other fields, it has evolved significantly with the digitalization of information and widespread of connected devices. Defined originally as the *art of writing in code*, or as we call it today *encryption*, cryptography is used almost everywhere information is being processed, stored, or transmitted. Apart from encryption, it is used to authenticate users, to secure digital and cryptocurrency or compute on data whilst keeping sensitive information secret, among many other security primitives.

The motivation for *quantum* cryptography is twofold. First, by utilizing quantum systems as information carriers, one can harness their new properties to obtain several advantages, or enhancements, in security. In quantum cryptography, security is a direct consequence of the laws of quantum physics, giving it a very strong foundation. Second, as quantum communication links and networks develop, these will need their own security protocols, specific to the quantum information that is manipulated. Quantum computing devices will also have unique security concerns. For example, the first quantum computers are likely to be available only by remote connection, and this may remain the case for the most powerful machines in a future where smaller quantum computing devices are commonplace. Delegating computations to remote devices has security implications, such as keeping certain information private and verifying the computation. Those tasks, called *blind* and *verifiable* quantum computing, will benefit from quantum communication capabilities, and will be discussed in Chapter 9.

A first step towards quantum networks

Networks of quantum computing devices and quantum-enhanced sensing are some of the most promising areas that will benefit from quantum communication capabilities. Despite their enormous potential, both require the most advanced quantum technologies, such as reliable long-distance quantum communication channels and ways to store quantum information. The required technologies and components are still very naïve and will require time and investment to come to maturity. Because of this, these applications are not expected before the next decade at the earliest[4].

Whilst this advanced technology is being developed, certain quantum applications are already possible on simpler quantum links. Quantum key distribution (QKD) is one such example, for which some protocols can already be implemented today. It is likely that if a quantum channel cannot be used to run certain QKD protocols, it will also be unable to serve as a quantum link for more advanced applications such as connecting quantum computers. This makes QKD a natural intermediary step as well as a valuable application on its own.

Encryption

To understand how quantum can enhance communication security, it is necessary to understand how we implement secure communication today. Classical information can be copied and amplified, in principle, at will. On the one hand, this is very useful to transmit signals at long distances, as we have seen already. On the other hand, an adversary who can physically access the communication channel can eavesdrop and copy the information traveling in it freely, for example by wiretapping a phone line. Because of this, sensitive information is never transmitted in *plain text*, but always in an *encrypted* form. Encryption scrambles the original, sensitive, information before it is sent over the channel. If all goes well, only the intended recipient can unscramble the encrypted message and recover the original information, in a process called *decryption*.

Encryption requires that the communicating parties, conventionally referred to as Alice and Bob, possess secret information that the eavesdropper, Eve, does not. Indeed, if Eve has the same information as the two parties, it is easy to see that she can decrypt the message directly, simply mimicking what Bob would do to decrypt. The secret information of Alice and Bob is called *shared secret keys* (or *symmetric* keys), i.e., a bitstring known only to Alice and Bob. Shared keys play the same role as two copies of a physical key giving access to a safe: the message is locked in the safe, which can only be opened again by someone who possesses the keys. Encryption plays the role of the safe in this analogy. An example of encryption is the *one-time pad*, which encrypts a message of n bits using a key of the same length: for each bit of the message, if the corresponding key bit is 1 Alice flips the message bit value (which is the sum of the two bits modulo 2, or XOR). The one-time pad is illustrated in Figure 6.1. Without knowing the key bit, every bit of the encryption looks completely random, hence does not reveal any information about the message. Bob, on the other hand, can obtain the message back again: he simply flips the bits back according to the key bit values.

Figure 6.1: An illustration of encryption using the one-time pad, requiring a key bitstring as long as the message. The message can be recovered by reverting the process, which is only possible with the key bitstring.

For practical reasons, amongst which is the long key length required, the one-time pad is rarely used. Instead, more efficient algorithms, such as the Advanced Encryption Standard (AES), take care of encrypting the message using shorter keys. Encryption is used every time *secrecy* is required; we rely on it when we send messages on our phones, when sending emails, to protect online transactions such as bank transfers, and for storing data or in more extreme situations such as military communications. Today, encryption is ubiquitous.

Distributing shared keys

Although encryption is well understood, a key challenge is to *distribute* the shared keys securely, often also called key *establishment* or *agreement*. Quantum key distribution (QKD) will be about this exactly, but first we will introduce existing classical methods to distribute secret keys.

Public-key cryptography

Not all is lost if the two parties do not have access to shared keys. In this case, one can rely on *public-key cryptography* (also called *asymmetric cryptography*), which is shown in Figure 6.2 and described by the following. One of the parties, say Alice, generates a *pair* of keys: one key that she makes public, the *public key*, and one key that she keeps secret to herself, the *private key*. Using the public key only, anyone (in particular Bob) can encrypt a message and send it over to Alice. Alice, who is the only one owning the private key associated to the public key that was used for encryption, has an extra piece of information making it easy for her to decrypt the message, whilst recovering the message is very hard for anyone without the private key. Coming back to our analogy, the public key allows anyone to close a padlock to lock a message, but it is very hard to re-open it except for the party possessing the private key. The public encryption scheme plays the role of the padlock, which can be used by anyone.

Such schemes rely on the assumptions of *trapdoor one-way functions*; functions that are easy to perform in one direction (to encrypt) but very hard to invert (to learn the message), unless one has an additional piece of information (the trapdoor, to decrypt). An example of such one-way function, which is used in practice in certain cryptosystems such as the famous RSA algorithm, is prime factoring: it is easy to multiply two prime numbers, but from the multiplied result only it is very hard to find the two primes again. By easy, we mean that the evaluation, or computation, of the function is

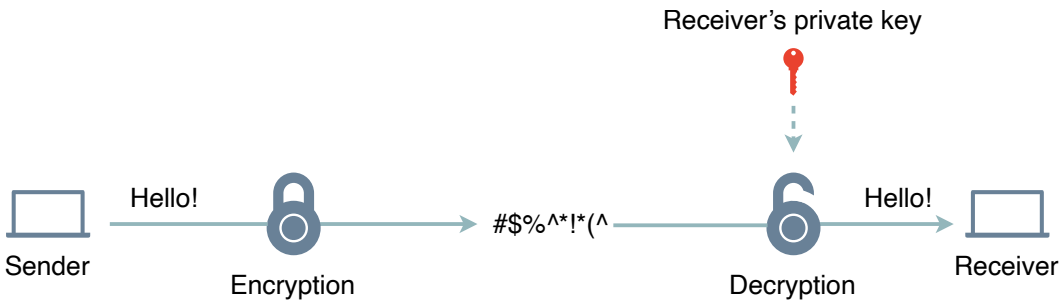


Figure 6.2: An illustration of public-key encryption. Encryption uses a public-key generated by the receiver, depicted here with a padlock. The receiver, owning the private key associated with the public key, is the only one able to decrypt the message. Public-key security relies on the hardness of inverting one-way functions.

efficient, hence can be done quickly on a standard computing device. As opposed to this, we call hard a computation that is so slow that, even on a very powerful computer, it is infeasible.

In practice, public-key protocols are mostly used to establish shared (or symmetric) keys between the two parties. In this case, the message encrypted using the public key simply is a random bitstring. After decryption, Alice recovers the bitstring, which only she shares with Bob. They can then use it in symmetric encryption, for example the one-time pad or AES, as shared secret key. Hence, the existence of a trapdoor one-way function implies that one can distribute shared, secret keys.

Public-key cryptography enables more than the distribution shared keys. Based on trapdoor one-way functions, one can also perform authentication, for example to make sure that a message indeed comes from the right person; imagine receiving instructions for a bank transfer that came from someone impersonating your bank. This is a more complex process involving a trusted third party and is called *digital signatures*. By signing a message with a private key allows anyone who uses the public key to verify that the message came from the right person – only someone with the additional piece of information (the private key) was able to build a valid signature. More precisely, a trusted third party (called a *certificate authority*) also certifies that the public key indeed comes from Bob, allowing Bob to digitally sign messages to anyone else trusting the third party. Digital signatures are the equivalent of signing a document by hand, in the presence of a notary validating the signature. We will mention quantum digital signatures in Chapter 9.

For a one-way function to be difficult to invert implies making both an assumption on the hardness of the underlying mathematical problem (factoring in our example) and over the computational power of the adversary. Indeed, if either an efficient algorithm is found for the inversion of the function or if an adversary becomes capable of dedicating enough computational resources to solve the problem in practice, even if inefficiently, the security of the protocol is compromised. Constant evolution in algorithms and computational power make it hard to predict how well those assumptions will resist the passage of time.

This issue is even more daunting because breaking the computational assumption in the future allows an adversary to *retroactively* compromise the secrecy of past communications. A malicious strategy known as *store now, decrypt later* can be applied; malicious parties may record data today in

the hope to break its encryption later, when the efficient algorithm or computational power becomes available.

The threat of quantum computing

As an example of the above, which is additionally relevant to quantum information, some quantum algorithms imply that certain one-way functions might be efficient to invert by future quantum computers, such as the factoring problem that we discussed. In that sense, what was hard for a classical computer might become easy for a quantum one in the future. Efficient quantum algorithms have already been discovered, the most famous being Shor's algorithm[33] which can be used for the factoring problem. If a ***cryptographically-relevant quantum computer*** can be built, i.e., one with sufficient quantum computing power to invert certain one-way functions in practice, an important part of the public-key protocols that we use today will be made obsolete. We come back to this point at the end of this section when we also mention ***post-quantum cryptography (PQC)***, which are public-key protocols based on computational assumptions believed to be hard for both classical and quantum computers. Quantum computing is only one example of why the landscape of computational assumptions is a moving one.

Quantum key distribution

Contrary to public-key cryptography, whose security relies on the assumed impossibility of solving certain mathematical problems, quantum cryptography and key distribution build on the limitations imposed by the laws of quantum physics. When implemented correctly, this means that one would need to violate fundamental physical principles to break a quantum protocol. This extreme level of security is often called *physical* and does not rely on the validity of a computational assumption. Even a futuristic adversary with immense computational power, quantum or classical, and any strategy that respects the laws of quantum physics can't break the protocol's security.

Following this approach, since certain processes are physically impossible when dealing with quantum systems, such as making clones of it or measuring them without disturbing and erasing their previous state, these also set *fundamental* limitations on the eavesdropper's capabilities. Such limitations on the eavesdropper are harnessed in ***quantum key distribution (QKD)***[34], but are also the foundation upon which quantum cryptography relies.

In the simplest *prepare-and-measure* QKD protocols, Alice sends Bob a sequence of quantum systems in a state that she keeps secret. Bob then measures the incoming systems to retrieve information from the transmitted state which they use to create a shared secret key. By later revealing a small sample of their data, Alice and Bob verify that Bob's measurement outcomes are indeed compatible with Alice's preparations: if yes, they traveled undisturbed. Indeed, a potential eavesdropper on the communication channel is left with a drastic choice: either leave the systems to pass untouched (hence obtaining no information from them) or interact with them at the cost of *disturbing* them (introducing errors that Alice and Bob will detect). The eavesdropper is also unable to make clones of the systems, in the hope to leave the original one untouched. All these observations would not hold if the transmitted information were classical. At the end of the QKD

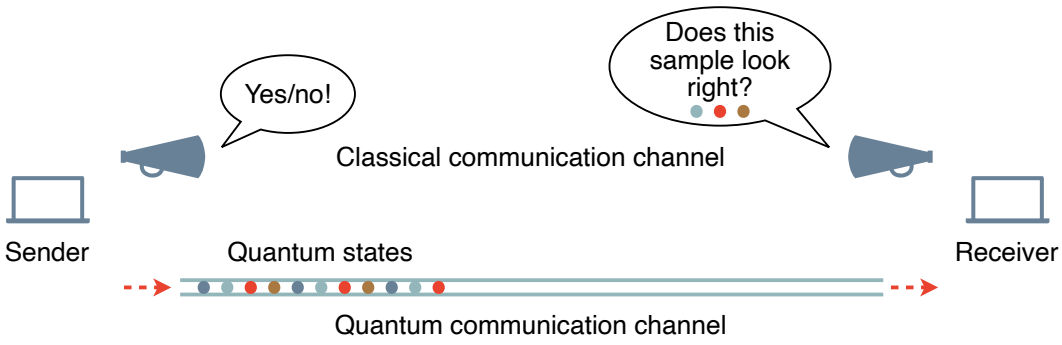


Figure 6.3: Illustration of a QKD protocol. The sender prepares quantum states which are sent to the receiver over a quantum communication channel. The receiver measures the transmitted quantum states and announces a sample of outcomes for verification. Verification can then be used to quantify channel errors and detect an eavesdropper.

protocols, Alice and Bob share a secret key which they can use for symmetric encryption, such as the one-time pad or AES which we mentioned.

A crucial aspect is that QKD needs *authentication*. The two parties need to be sure that they are talking to each other and are not being impersonated - imagine establishing a shared key with the wrong person! This implies that the parties require a *pre-shared key*, which the QKD protocol expands into a larger shared key without relying on the assumptions of one-way functions as in public-key cryptography. Alternatively, the user can use public-key digital signatures for authentication, in which case they rely both on a computational assumption and a trusted third party. In this case, despite making a computational assumption, it is only required to remain valid *during* the execution of the protocol, which is typically a few seconds at most. Authentication is different from encryption; there is no value breaking it later since the parties will have already finished using this part of the communication protocol. This is called everlasting security and makes it invulnerable to the *store now, decrypt later* strategy. The quantum enhancement in key expansion and everlasting security are impossible to achieve with only classical resources.

Challenges

The main challenge of QKD comes from the fact that unavoidable imperfections in preparing, transmitting, and measuring the quantum states are very hard, if not impossible, to distinguish from an eavesdropper's actions. Because of this, sources of error need to be attributed to eavesdropping and QKD protocols require very high system performance. Indeed, if too much noise is present, the protocol is aborted due to possible eavesdropper interference.

QKD systems today are very limited both in the distance over which they can be implemented, as well as their real-world security capability. Because of the challenges outlined in Chapter 5 making the sending and receiving of quantum states over large distances very difficult, QKD for now is limited to transmission over a few hundreds of kilometers at most. Adding to this, as noted for example in US and UK recommendations[35,36] because of implementation imperfections, engineering and integration challenges, aging and environmental effects, and lack of vulnerability research, QKD is still very much in the research phase. Because of this, both governments recommend against

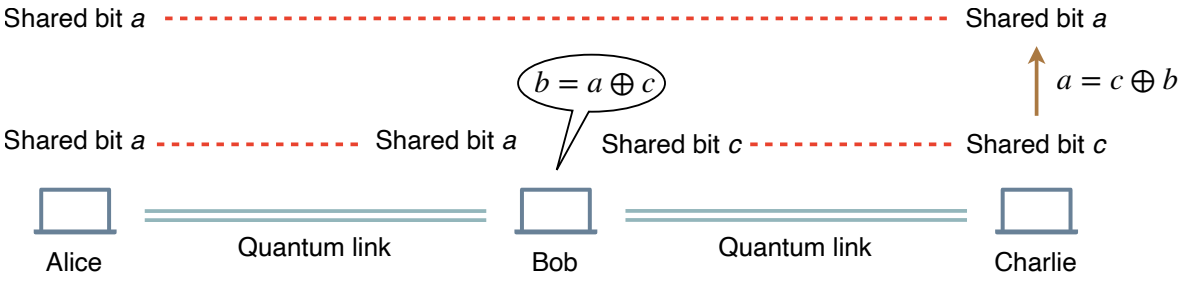


Figure 6.4: An illustration of two parties (Alice and Charlie) connected to a trusted node (Bob) through independent quantum links. Bob announces the bit result $b = a \oplus c$ while keeping a and c secret. Charlie computes $a = c \oplus b$ and now shares the value of a with Alice. Bob needs to be trusted because he also has access to the shared bit.

using QKD for commercial or military purposes. We note that there is nothing prohibitive in these limitations of today's QKD, as exhibited by both governments investing and supporting QKD research in other institutional efforts (e.g., academia). We come back to those challenges when discussing future quantum cryptography, which offers novel solutions such as *device-independence*.

Trusted repeaters

Point-to-point QKD links can be extended using trusted repeaters, which are fundamentally different from quantum repeaters which we introduce in Chapter 8. If Alice and Bob are connected by a QKD-capable link, and Bob is similarly connected to Charlie, Bob can serve as a trusted node to connect Alice and Charlie. This process is demonstrated in Figure 6.4. The advantage of this approach is to break the total distance into shorter sections. The idea is as follows. If Alice and Bob have a bit a of shared secret key, and separately Bob and Charlie have a shared bit c, Bob can simply announce in public the value of bit $b = a \oplus c$ where $\oplus$ is the XOR operation. Note that bit b does not give any information about individual bits a or c, hence why it can be announced publicly. Charlie, in possession of bits c and b, can then obtain bit a using that $a = c \oplus b = c \oplus c \oplus a$. The drawback of this approach is that Bob also is in possession of bits c and b, hence also knows the final key bit a. Because of this, Bob needs to be trusted and there is no end-to-end security.

Device-independence

One of the most important vulnerabilities of a cryptosystem, quantum or not, is a mismatch between its theoretical description and its actual implementation. If a cryptosystem is implemented correctly, with hardware that functions as promised, then all goes well. But what if this isn't the case? This vulnerability is especially relevant for quantum technologies that are comparatively less mature than classical ones. As we have seen above, the US and UK governments advise against using QKD today because of implementation imperfections, engineering and integration challenges, aging and environmental effects, and lack of vulnerability research[35,36].

Device-independent (DI) quantum cryptography offers a solution to several of these issues. Instead of a precise description or model of the hardware, in a DI protocol all the quantum parts of the system

are seen as black boxes whose functioning is untrusted. The idea is to use the observation of unique quantum behavior to verify the black boxes' internal functioning, instead of assuming its correct implementation. The protocol's security is then not dependent on a correct model or implementation, hence the name device-independence. Because of this very strong security promise, DI protocols such as DI-QKD are regarded as the gold standard of cryptography: no attack can use a mismatch between theory and implementation of the quantum hardware.

To understand how this is even possible, we turn again to quantum entanglement. As we have seen, measuring two systems in an entangled state can generate strong quantum correlations that are impossible to obtain with classical resources. Certain quantum correlations go even further: they *self-test* by discarding all but one strategy to be generated. In other words, when observing these self-testing correlations, one can obtain knowledge of both the quantum state and the measurements that were made on it - there is no other way to obtain those correlations! Device-independent protocols exist to verify the unpredictability of the outcome of devices (to generate cryptographic keys for example), quantum computations or quantum properties such as entanglement. Because of this, device-independent protocols are useful beyond cryptography only, for example as a very powerful hardware characterization technique. This last observation is especially relevant when testing components and functionalities of quantum communications for properties such as fidelity.

We note that device-independent protocols still rely on a few minimal assumptions, such as the ability to synchronize clocks or that the classical hardware functions as promised. Device-independent QKD protocols were recently demonstrated for the first time in lab conditions[37], showcasing their future viability. For now, despite holding great potential, due to the challenge of reliable entanglement distribution and requirement for even higher system performance, device-independent QKD is still in its research phase.

Recent developments

Quantum key distribution is one of the most mature applications in quantum communications. Many different countries and institutions have proof-of-concept demonstrations and commercial QKD systems are readily available by a few providers. However, there are many challenges in achieving useful key rates over long distances.

Fiber-based systems

One promising area of research in secure quantum communications is twin-field QKD (TF QKD) for its long-distance rate-loss scaling. In the lab, TF QKD has been demonstrated over a 658 km ultra-low-loss fiber[38] with an average loss of 0.161 dB per km across the channel, including connections, and recently scientists have shown the potential of expanding to over 830 km of fiber[39]. In the real-world, quantum key distribution has been demonstrated over a 511 km long fiber link between two cities, without a quantum repeater[40].

Device-independent QKD promises enhancements in security but is still very much a future technology with the first successful in-lab demonstrations achieved only recently[37]. However, there has been growing research into measurement-device-independent QKD (MDI QKD), in which

the measurement system, the most often attacked and arguably most vulnerable part of the QKD system, remains untrusted. MDI QKD has been achieved over 404 km of ultra-low-loss fiber[41].

Satellite-based systems

Today the furthest distances achieved in QKD proof-of-concepts are via links with the Micius satellite, an LEO satellite with quantum capabilities[42]. Onboard the satellite are advanced optical components for generating pairs of photons entangled in polarization and sending these to ground stations. To date, the project has achieved long-distance entanglement distribution over 1200 km[43], prepare-and-measure QKD between satellite and ground station over 1200 km[42], generating keys used to secure a video-conference between China and Austria[44], and enabled entanglement-based QKD between two ground stations 1120 km apart[45], albeit with only 6 bits of final secure key each time the complete protocol is run.

Post-quantum cryptography

To mitigate the threat that quantum computing poses to the security of certain public-key schemes in the future, it is also possible to rely on one-way functions that are assumed to be hard to invert as well for a future cryptographically relevant quantum computer. For example, instead of relying on the hardness of factoring, one can rely on hard problems over lattices such as finding the shortest or closest vector. Such public-key algorithms are called post-quantum secure (sometimes also *quantum-safe* or *quantum-resistant*). Contrary to QKD, PQC still relies on a hardness assumption for as long as secrecy is needed but offers higher compatibility with existing infrastructure and offers more than only key distribution (called key *establishment*). For example, post-quantum digital signatures are proposed, which may even be very useful in a QKD protocol with *everlasting* security that we discussed. In 2017, the National Institute of Standards and Technologies (NIST) asked for PQC algorithms proposals for both key distribution and digital signatures, which were then made publicly available for analysis, leading to first draft standards in 2022 that are still open for comments[46].

There is currently an intense debate on which of PQC or QKD will be used for each different application in the future, when QKD may be made practical and achieve real-world security. As said, future developments such as the ability to run device-independent protocols and vulnerability analysis of QKD systems will help in this regard.

NASA's SCaN

We have seen in Chapter 5 that the SCaN program roadmap includes the development of advanced components, such as high-performance single-photon detectors and sources, which will advance many applications, including quantum-enhanced security. With better sources, detectors, and links, we can overcome existing barriers to loss and increase secret key rates in QKD systems for example. Later in Chapter 8, we introduce another technological breakthrough that could enable long distance and networked quantum security: quantum memories. The development of networks is supported by NASA's qEDISON proposal to build quantum links with both low- and medium-Earth orbit satellites

distributing entanglement. The fact that these links are built on entanglement is doubly beneficial for security applications. First, it will allow long distance quantum communications beyond the rate-loss limit, currently the main challenge of QKD, as well as circumventing the problem of line of sight due to the earth curvature. Second, entanglement also enables device-independent security applications, offering unprecedented levels of security. Indeed, QKD but also more advanced applications such as quantum money or digital signatures, which we cover in Chapter 9, will be possible.

As mentioned, those quantum links are as much an excellent testbed for security applications and their development as these applications are a necessary test for the links themselves. For example, demonstrating device-independent QKD enabled by entanglement distributed by satellites, we will be able to characterize and quantify the quality of said link and other components such as the measurement apparatus. Entanglement is also the underlying resource for future functionalities such as quantum repeaters, which the SCaN program roadmap aims to support by making satellite-based entanglement distribution as future-compatible as possible. Finally, such links offer a very useful testbed for novel applications beyond the ones we have mentioned, supporting research and development beyond what we can think of today. We will take a closer look at the work NASA's SCaN program is doing towards the development of quantum networks in Chapter 8.

7 Quantum Metrology

Quantum metrology is poised to play a pivotal role in building and connecting quantum devices in a large network. When synchronization of independent photons carrying quantum information through a network must be precise to sub-picosecond time scales, understanding precision measurement limits is critical. Moreover, understanding the dynamics of distributed quantum systems, their characterization, and how they will be integrated in the future, will enable opportunities for more exploratory advances in quantum metrological applications.

To this end, with metrology being the study of precision measurement, quantum metrology aims to determine the limit of precision measurements for systems using quantum resources. As such, quantum metrology represents the *ultimate limit* for which any precision measurement can be made.

For any measurement, the limit is established as a *parameter estimate* governed by the noise fluctuations of components within the measured system. In vacuum, *quantum fluctuations* of the electromagnetic field contribute to noise factors which prohibit absolute measurement certainty, thus adding constraints where quantum measurement is applicable. A quantum measurement is realized as an estimate of an unknown *quantum* parameter; ***quantum metrology*** is the study of how precise this estimate can be.

In this chapter, we give a brief overview of fundamental concepts in quantum metrology applicable to future distributed systems. Additionally, several applications that highlight the promising technological advancements made possible by quantum metrology are explored.

Limits of measurement

Quantum metrology aims to determine the limit of precision measurements for systems using quantum resources or exhibiting quantum phenomena. As noise is an intrinsic property to any quantum measurement, it is prudent to discuss how quantum metrology allows for noise reduction in a variety of quantum applications.

The ***standard quantum limit (SQL)*** represents the precision limit of measurement for optical parameters within the system when only considering individual resources. For example, in the case where photons are used one at a time. However, the SQL does not hold when considering *entangled* quantum systems. Quantum metrology achieves the ultimate theoretical limit of precision for any measurement – the ***Heisenberg limit***, which we introduced in Chapter 2. By using entangled states of light, we can make measurements with an uncertainty below that of the SQL. To understand how we can achieve this, we will first introduce how optical measurements can be made.

Optical interferometry

One technique which has played a significant role in precision measurement is interferometry. Since its invention by Albert Michelson in the mid-1880s, the interferometer has played a crucial part in measurement. One of the fundamental models used for realized metrology experiments is the

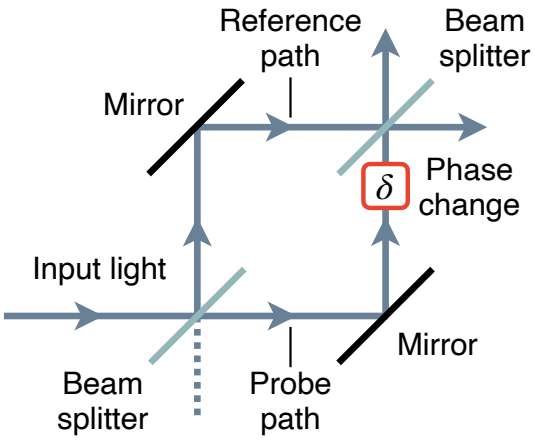


Figure 7.1: A Mach-Zehnder interferometer (MZI) which is commonly used in metrology. A sample of interest is placed in the probe path and induces a phase change which can be measured.

Mach-Zehnder interferometer (MZI), an optical setup designed to study the interference of light waves[47], which is shown in Figure 7.1.

A light beam enters the interferometer and is split into two directions by a beam splitter. One of the emerging paths will serve as a probe and experiences a change in phase, δ. This phase change results from the interaction of the light in the probe path with some medium or material we wish to measure. Therefore, the phase change acts indirectly as the parameter that we wish to estimate, and which we could not otherwise measure directly. The light from the probe path then interferes with the *reference* light from the other path at a second beam splitter. The result of the interference is that the encoded phase change will be converted to a change in the intensity of the output light, which can then be measured directly. If the phase (or other parameter of interest) is to be measured as accurately as possible, there must be a way to reduce the statistical noise fluctuations inherent in the phase, thus improving the measurement.

Over time, this model has been used to study interference effects of many quantum systems which exhibit wave-like properties. It was shown in 1981 that vacuum fluctuations exist in unused ports of the interferometer[48]. These vacuum fluctuations contribute to phase measurement limits for the interferometer. Phase-noise measurement is ubiquitous in quantum metrology.

The precision with which we can measure the phase change, when considering classical light, is given by the SQL. This limit depends on the number of optical resources used. For example, consider the case where we use N photons from a laser as the input for our interferometer. The imprecision in estimating the phase change, or uncertainty in the measurement, will scale as $1/\sqrt{N}$. In other words, the measurement uncertainty decreases with the square root of the number of photons used.

Squeezing and sub-SQL measurement

So how does one beat the SQL with quantum states of light? Using a quantum optical phenomenon known as ***squeezing***[49], one can reduce quantum noise fluctuations in the phase measurement beyond the SQL, resulting in sub-SQL measurement. Squeezing refers to the manipulation of intrinsic properties of a quantum system, a photon, for example.

In Chapter 2, we introduced the uncertainty principle which governs the precision to which we can measure certain properties of quantum systems. The limit is given by the equation $\Delta x\ \Delta p \geq \hbar/2$ where x and p are the properties we would like to measure. Squeezing is the observation that we can satisfy the uncertainty principle by *increasing* the uncertainty in one property, while allowing the uncertainty of the other to *decrease*. Light is described by an electromagnetic field that has an amplitude and a phase. Increasing the uncertainty in amplitude allows the uncertainty of the phase to decrease, resulting in a phase-squeezed state. Conversely, decreasing the noise in the amplitude would result in an amplitude-squeezed state. Quantum optical squeezing allows quantum-enhanced measurement precision for sensing and imaging referred to as super-sensitivity and super-resolution.

Referring to the Mach-Zehnder interferometer above, inputting a phase-squeezed state into the interferometer introduces more noise into the amplitude component of the light. As the measurement of the amplitude is not of interest, increasing the noise in this component allows for more precise measurement of the phase change.

Considering again the SQL, but instead when using our quantum resource of squeezed light. The precision of the measurement can now scale with $1/N$, which is a $1/\sqrt{N}$ improvement meaning we can achieve a sub-SQL precision. This achieves the same precision as a measurement with classical light while using fewer optical resources.

Various types of interferometers, such as Michelson and Sagnac, can also be used for optical metrology, where squeezing allows for sub-SQL measurement of electromagnetic fields, distances, rotations, plasmonic surface characteristics, and more.

LIGO and gravitational-wave detection

In 2015, scientists detected gravitational waves for the first time using the Laser Interferometer Gravitational-Wave Observatory (LIGO) which comprises two, very large Michelson interferometers. One observatory is in Hanford, Washington and the other is in Livingston, Louisiana (shown in Figure 7.2). Each observatory uses a laser directed along two, 4-kilometer paths towards mirrors to detect these tiny ripples in the fabric of space-time. Since gravitational waves cause space itself to stretch in one direction, whilst simultaneously compressing in the perpendicular direction, one path of the interferometer is elongated while the other shrinks, then vice versa, continuously as the wave passes across it. The longer the light path, the larger the phase change. For LIGO, this change in distance is measured to be 1/10 000$^{\text{th}}$ the width of a proton, equivalent to measuring the distance to the nearest star to our solar system (4.2 light years away) to an accuracy smaller than the width of a human hair[50]. The gravitational waves that were ultimately measured were caused by two black holes colliding 1.3 billion years ago. Until recently, the measurements at LIGO have been limited to the SQL. In 2023, LIGO enhanced its measurement capabilities using squeezed light to reduce noise and increase precision measurement across the entire range of gravitational wave frequencies of interest[3].

Although LIGO is extremely sensitive, a space-based system would be able to detect waves at even lower frequencies and detect different types of sources. NASA is working closely with the European Space Agency (ESA) to develop a concept for a space-based gravitational wave observatory[51].

Figure 7.2: LIGO observatory in Livingston, Louisiana. **Image credit:** Caltech/MIT/LIGO lab[50].

Quantum parameter estimation

When measuring unknown parameters of systems, it is imperative that estimates be reliable; for future technologies requiring quantum networks, for example, improper estimates for quantum parameters can lead to potentially significant operational issues.

An example of parameter estimation from classical physics is determining, to best precision, the strength of an unknown local magnetic field from many measurement samples of charged particle dynamics. The most precise measurement given by classical estimation theory is the lower limit of the ***Cramér-Rao bound (CRB)***: a lower bound on the variance of any unbiased estimator.

An unbiased estimator is one that, given a sample of events, produces a parameter estimate which is known to converge to the true parameter value for a large sample. Therefore, in the limit of infinitely repeated sample measurements from a set of data, the unbiased estimate for any given sample produces the expected result. For a finite number of samples, the difference between the estimate and the true value can be bounded. This means that this estimator, together with error bounds, can be used to evaluate a parameter.

Classically, the ***Fisher information (FI)*** describes how much information about the true parameter can be obtained from a sample measurement and is inherent in the CRB. Thus, if an estimator satisfies this bound, it is considered an ideal estimator for the unknown parameter of interest.

Determining the limit of measurement accuracy for systems exploiting quantum resources is the goal of ***quantum parameter estimation (QPE)***: the mathematical framework of quantum metrology. The fundamental limit in precision measurement is given by the ***quantum Cramér-Rao bound (QCRB)***[52].

Like classical estimation, inherent to the QCRB is the ***quantum Fisher information (QFI)***, which bounds the achievable precision in parameter estimation with a quantum system[53].

Informally, quantum Fisher information can be thought of as the sensitivity of a quantum state to changes in an unknown parameter of interest and has an inverse relationship to the measurement uncertainty; a larger QFI gives us more confidence that our estimate agrees with the actual value of a parameter.

Quantum parameter estimation involves preparing a quantum system in some known, well characterized, quantum state, again referred to as the *probe*. The difference now is that rather than using a classical probe such as a light beam with some intensity, we now require the use of a quantum system such as a single photon with a specific polarization. As before, the probe is allowed to interact with an unknown system of interest and, after the interaction, information about the desired parameter is *encoded* onto the probe state. If the dynamics of the interaction are known, information about the unknown parameter can be deduced by measuring the probe and comparing the result to the initial state.

If multiple quantum systems are entangled, then these systems collectively make up a single probe state where a sub-SQL measurement can be made. The same process as above is applicable to large, entangled states composed of multiple quantum systems. But what if measurements need to be made simultaneously on several parameters of a system which are incompatible? This is the role of ***quantum multi-parameter estimation (QME)***.

Multi-parameter estimation

Quantum metrology aims to achieve high-resolution and highly-sensitive measurements of physical parameters using quantum theory. Ideally, this would be possible no matter the type or number of parameters in a system.

Estimation is attainable for a single parameter, but for many parameters, the limit to our precision of given measurements may be different depending on the parameters. The optimal measurement for a given parameter might not result in an optimal measurement for all parameters if they are incompatible, i.e., there is a trade-off imposed by the uncertainty principle.

We combine the quantum Fisher information of single parameters when performing simultaneous measurement of multiple parameters. A multi-parameter precision measurement is limited by the Helstrom bound[54], which is the quantum Cramér-Rao bound generalized to QME[55]. Although challenging to evaluate, this bound represents the best precision result attainable for systems with large parameter number and global measurements[56].

Atomic clocks

As we have seen in previous chapters, electron states in atoms are associated with different energy levels, and during transitions between these discrete levels they interact with a very specific frequency of electromagnetic radiation. This results in a reliable frequency reference when trying to measure frequencies of other oscillating systems.

Atomic clocks can be used to precisely measure the passage of time. In fact, the second itself is defined by an atomic clock, taking the fixed numerical value of the frequency related to one of the ground state transitions of the cesium-133 atom. NIST's cesium fountain clock named NIST-F2, measures time with an uncertainty of 1 second in 300 million years[57].

The accurate timekeeping of atomic clocks is the foundation for the system of International Atomic Time (TAI) governed by a collection of atomic clocks around the world. Other systems, such as Coordinated Universal Time (UTC), go further to account for changes in Earth's rotation to within one second. Atomic clocks are also used in satellite networks for navigation, such as the United States' GPS, where the smaller the error in time measurement, the smaller the error in distance.

The NIST-F2 is a type of *microwave* atomic clock, where microwaves are used to put the spin of an atom in a superposition state, and the atomic spin is allowed to precess in a particular way. The precession of the spin quantifies its change in pointing direction (think of a rotating arrow) and this angular displacement from the spin's original position is known as the *phase angle*. This phase is the quantum parameter to be measured, and the accuracy of its measurement depends on the number of spin measurements taken and the time allowed for each spin precession.

More recently, *optical* atomic clocks, which interact with the atoms using light rather than microwaves, have been developed which offer even higher stability and reduced uncertainty. Those based on trapped ions, in which a charged ion is trapped by relatively weak electric fields and held fixed within a vacuum system, suffer very little disturbance to their atomic absorption 'clock' frequency. Clocks such as these can achieve uncertainties orders of magnitude smaller than those based on cesium and could one day redefine the second. As well as tests of fundamental physical theories, optical atomic clocks will in future be useful in the development of quantum sensing and synchronization of high-speed quantum networks.

Metrology for communication

Central to building large-scale quantum communication networks will be the subsystems and components that will generate, process, and measure quantum information. As these systems inherently deal with quantum states, quantum metrology will be instrumental in ensuring that devices are operating as expected.

Devices in a quantum network require measurements to maximum precision of unknown quantum states to confidently store, process, and transmit information. It therefore follows that quantum metrology plays a key role for future quantum communication platforms. As we have now seen, for any measurement there is a limit on the precision to which we can estimate an unknown parameter due to quantum noise fluctuations contributing to the measurement result. We have also seen how single photons will be widely used to distribute quantum information across networks. It is therefore necessary that we have detectors that are sensitive enough to measure at extremely low energy levels. This will be important to ensure that we are encoding the information correctly but also that we are reading (measuring) that information correctly once received. The quantum links used to distribute photons will exhibit noise and loss that will cause errors in any quantum communication protocol. A good understanding of this process is essential to building a robust network. As quantum

networks advance, it will be critical to develop our understanding of how light interacts with atoms, for which quantum metrology will be key.

Beyond being instrumental in building networks, quantum metrology itself will benefit from large quantum communication technologies. Distributed networks of entangled quantum states can be used as a sensor array to enable more enhanced gravitational sensors or synthetic apertures for astrophysics. However, arrays of quantum sensors can be incredibly fragile due to the brittleness of quantum entanglement. Losing even a single photon can destroy the entire state. It will be important for future quantum sensor networks to overcome these errors so that enhanced measurements can be achieved in a noise-tolerant way. In the following chapter, we will see how new quantum protocols can overcome loss to distribute entanglement over large distances.

8 Quantum Networks

In the early 1960s only large mainframe computers existed, each with a separate set of users with terminals either hard-wired to the computer or connected via a local phone line. To transfer data from one computer to another, you had to physically move it by tape. In 1967, the ARPANET project, a US-wide network of communicating computers, was announced, laying the foundations for today's Internet. Now, billions of computers, small devices, and sensors are communicating and exchanging digital bits of information around the world.

Our motivation to develop quantum networks is the same as for classical networks: connecting people, computers, sensors, and databases in distant locations. At the heart of quantum networks is entanglement, our uniquely quantum resource that enables us to implement new quantum communication protocols and extend the reach of our quantum links.

This chapter will introduce some of the building blocks of quantum networks. These new networks comprise a myriad of different devices in the pursuit of distributing entanglement along both fiber and free-space links. To connect these devices together, we will introduce how quantum information can be converted between different physical encodings to ensure seamless compatibility across a wide range of necessary components. Finally, we will describe the progress of quantum networks around the world and how NASA's SCaN program is poised to play a vital role in their development.

Entanglement distribution

Quantum entanglement is a fundamental resource for any future quantum network. Therefore, distributing entangled states between nodes, or users, is of critical importance. Quantum states exchanged between nodes of a network may be individual qubits carrying one element of quantum information, or they may be part of a larger quantum state. For example, we may wish to distribute an entangled state which spans multiple nodes in a way that no shared classical state can.

Any communication channel will experience loss causing the signal intensity to decrease as it travels along the channel. Beyond a certain distance, the signal will be so weak that it can no longer be reliably measured. For example, in modern telecommunications, bright laser pulses are used to encode information which are then transmitted over an optical fiber. After only 15 km of fiber, the signal intensity has reduced by half so to reach further distances we need to overcome this loss. This is achieved by introducing a classical repeater – a device that measures the signal and then produces a new, strong signal that encodes the same information. Networks are divided into shorter segments connected by repeaters which maintain signal integrity.

Naturally, quantum communication is also impacted by loss, but the effect is far more detrimental. As we use single photons to encode our quantum information, if the photon is lost then the information is lost with it. However, the no-cloning theorem, that we introduced in Chapter 2, prohibits us from measuring the quantum state and creating a replica. Therefore, we need a new method to overcome the loss to reach longer distances – for that we must use entanglement to create ***quantum repeaters***.

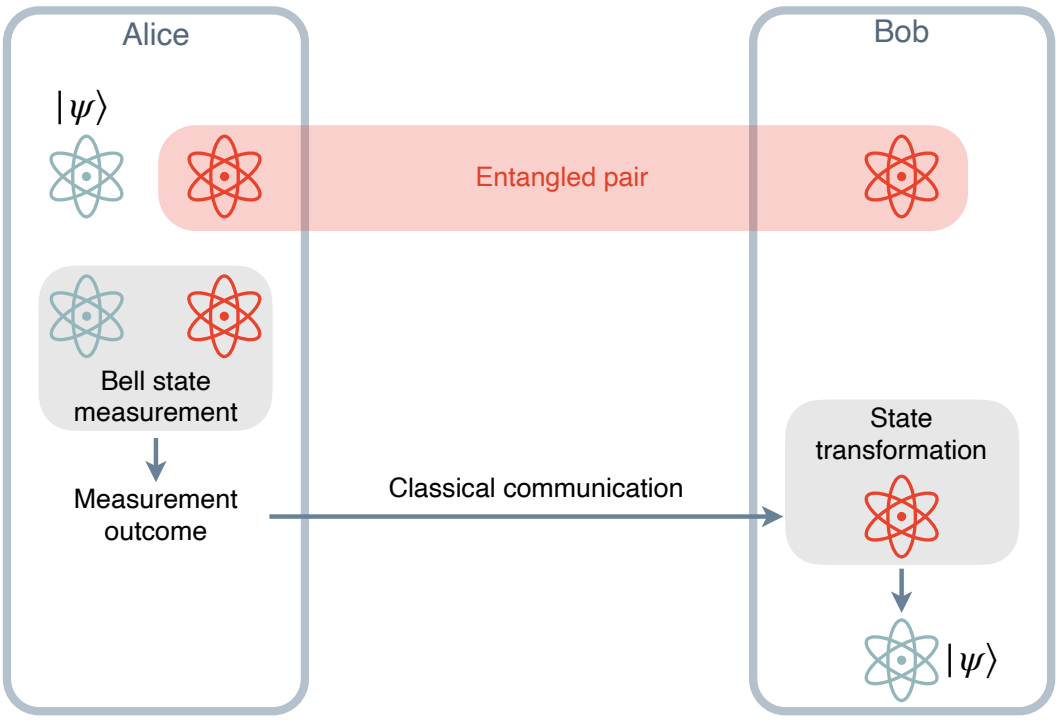


Figure 8.1: Quantum teleportation protocol. Alice and Bob share and entangled pair of qubits and Alice has the state $|\psi\rangle$ that she would like to send to Bob. Alice performs a Bell state measurement on the qubit that she would like to send and her half of the entangled pair. She sends the measurement outcome to Bob over a classical channel. Based on the measurement outcome, Bob performs a state transformation on his qubit, which transforms his qubit into the state $|\psi\rangle$.

Teleportation

To understand how we might construct a quantum repeater, we first describe how we can transfer quantum information using entanglement through a process called ***teleportation***, outlined in Figure 8.1. This process circumvents the no-cloning theorem by directly transferring the quantum information from one particle to another without making a copy.

Imagine two people, Alice and Bob, each have one half of an entangled state. Alice would like to send some quantum information, encoded in the quantum state $|\psi\rangle$, to Bob but knows that by sending the information over a lossy channel it is unlikely to arrive. Instead, Alice encodes her information into a qubit and performs a joint measurement with her half of the entangled state. The measurement is called a ***Bell state measurement*** and collapses both of Alice's particles into an entangled state. However, this also causes Bob's half of the initial entangled state to collapse. By sharing the result of the measurement, Bob is able recover exactly the quantum information that Alice encoded – the information has been *teleported*. They can continue this process for each quantum bit that Alice wants to send.

Alice and Bob can be very far apart, but quantum teleportation does not allow for information to be sent faster than the speed of light. Only once Bob receives the result of the measurement, by communication over the classical channel, can the quantum information be reconstructed. Provided we can distribute entanglement over long distances, quantum teleportation can overcome the challenge of channel loss to reliably transmit quantum information.

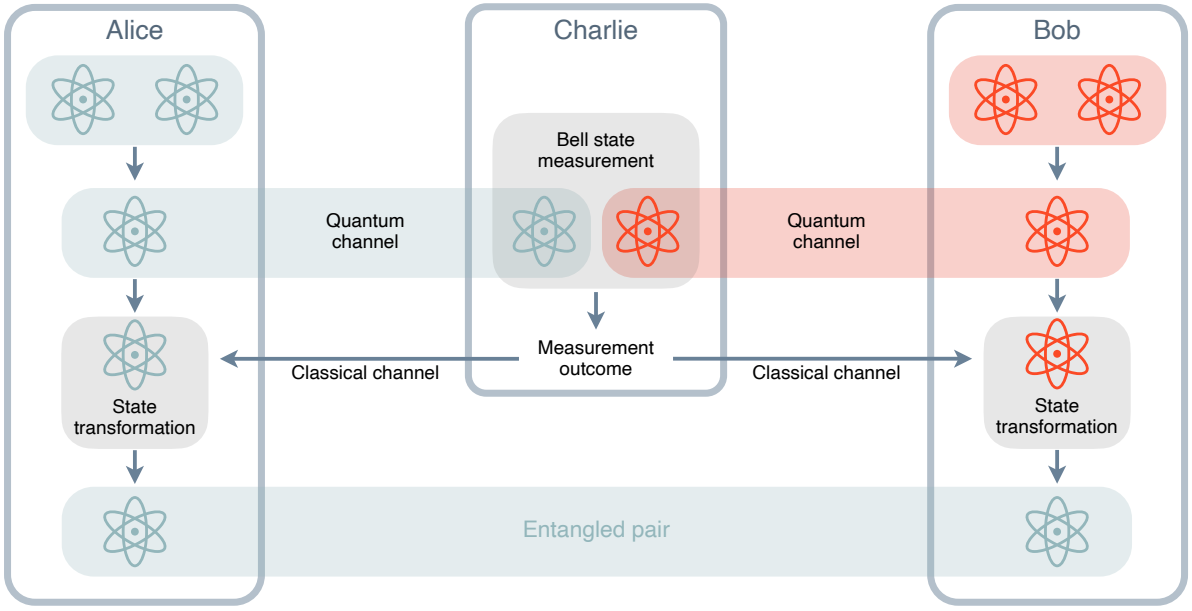


Figure 8.2: Entanglement swapping protocol. Alice and Bob each have their own entangled pair of qubits. They each send one qubit from their pair to a intermediate node, here called Charlie. Charlie performs a Bell state measurement and sends the measurement outcomes to Alice and Bob. By performing state transformations based on the measurement outcome, Alice and Bob now share an entangled pair of qubits.

Entanglement swapping

To understand how we can distribute entanglement, we first need to introduce ***entanglement swapping*** which builds on the concept of teleportation. However, instead of quantum information being sent, it is instead the entanglement itself that is transferred or *swapped*. This protocol is shown in Figure 8.2.

Consider now that Alice and Bob each have a pair of entangled particles. They each send one particle from their entangled state to an intermediary node, Charlie, where a Bell state measurement is performed. The measurement outcome is shared with Alice and Bob who perform state transformations based on the outcome. This leaves the particles shared between Alice and Bob in an entangled state. We have created entanglement between particles that have never interacted!

The process of entanglement swapping separates establishing entanglement from sending quantum information. Alice and Bob can repeat the entanglement swapping process until it is successful and only then send quantum information through teleportation. This allows us to overcome channel losses that would otherwise prohibit quantum communication over large distances.

Quantum repeater

Finally, we can combine teleportation and entanglement swapping to transfer quantum information over long distance. As with classical repeaters, the channel is split into many smaller sections which connect devices that generate entangled particles. In successive rounds, the entanglement is swapped between adjacent nodes. After sufficient rounds, the two end nodes will be entangled and quantum teleportation can be used to send a qubit. This process is shown in Figure 8.3.

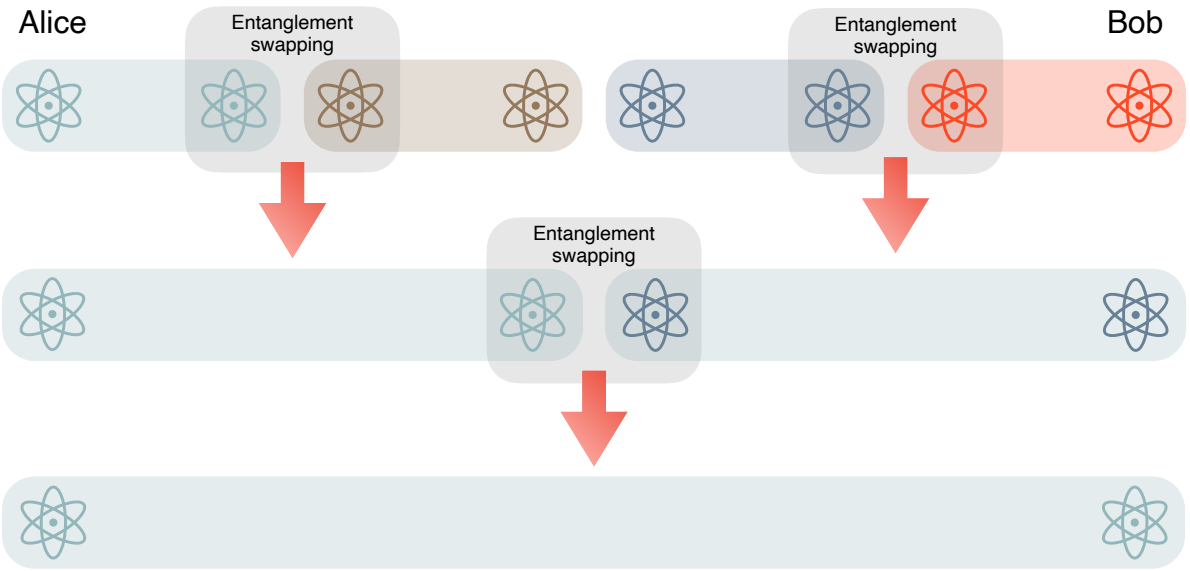


Figure 8.3: Quantum repeater protocol. By using many entangled pairs and entanglement swapping, we can break the channel into smaller sections to overcome channel loss. Entangled pairs are shared between adjacent nodes and entanglement swapping is performed until Alice and Bob share an entangled state. This can then be used for quantum communication, such as sending a qubit through teleportation.

Quantum repeaters may look like a cumbersome way to send quantum information because long links require many rounds to distribute the entanglement. However, separating the processes of establishing entanglement and sending quantum information overcomes the channel loss.

Entanglement distribution with satellites

To achieve global quantum connectivity, we will need to distribute entanglement over large distances. Satellites are well suited for this task as one satellite alone can connect ground stations thousands of kilometers apart.

There are three different architectures[58] that we can use to distribute entanglement between ground terminals which are shown in Figure 8.4. The first is a dual downlink where the satellite has an onboard entangled photon source which transmits to two separate ground stations. This method directly transmits entanglement to the ground stations and does not require synchronization between the ground terminals and the satellite. The second architecture is a dual uplink where entanglement is generated at each ground station and photons are transmitted to the satellite. The satellite performs a Bell state measurement and relays the outcome back to the ground station. Through entanglement swapping, the ground terminals now share an entangled state. This requires that the photons arriving at the satellite are synchronized. Finally, we can consider a hybrid where one ground terminal has an entangled photon source that is shared through an uplink to the satellite. The satellite acts as a passive routing device to re-transmit the photon to the second ground station. Again, we no longer need to synchronize the satellite to either of the ground terminals.

High-rate entanglement distribution requires precision synchronization of interacting photons originating from different entanglement sources in different locations. This is a particular challenge for

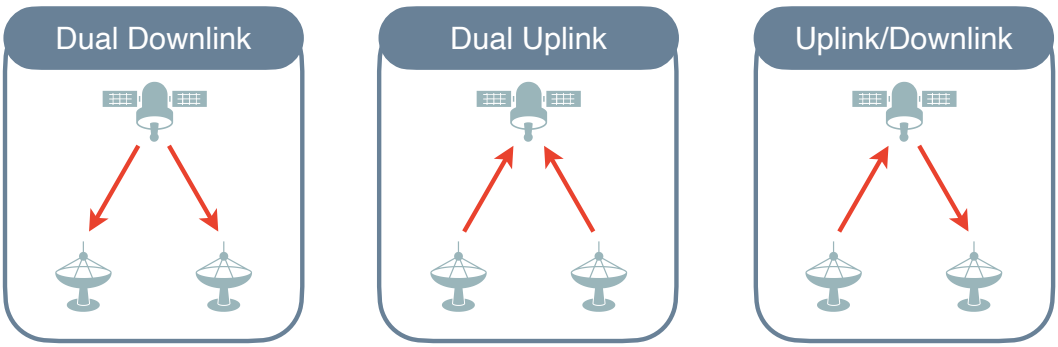


Figure 8.4: Three space-based entanglement distribution architectures each with different advantages, disadvantages, and design considerations[58].

satellite-based entanglement distribution, where photons need to be synchronized over potentially thousands of kilometers where relative motion, channel effects, and propagation delay need to be considered. In a collaborative effort between NASA's SCaN and MIT Lincoln Laboratory[58], a quantum networking testbed is exploring a precision synchronization method for free-space entanglement distribution. The technique is considered for sources at two different ground stations, interacting at a satellite in a dual-uplink scenario. Photons from entanglement sources at the ground stations interact in a Bell state measurement on the LEO satellite. Each source also provides a synchronization signal to the satellite, and synchronization is achieved using a control loop in which timing information is fed back to the ground stations.

As proposed by NASA's SCaN team, an LEO platform such as the International Space Station (ISS)[4] could distribute entanglement between ground stations as far as 1200 km apart – similar to the record distances achieved by the Micius project[42] highlighted in Chapter 6. This is done using entanglement swapping where a pair of entangled photons is generated on the ISS, and another is generated at a ground station. One photon of each pair is sent to undergo a Bell state measurement, creating an entangled link between the ground station and ISS. The remaining photon on the spacecraft could then be sent to another ground station and the process repeated to establish connections between devices on Earth without a direct link. A spacecraft in a higher orbit could connect ground stations much further apart, but would require high clock-rate sources, extremely high pointing accuracy in the telescopes, and large diffraction-limited apertures to overcome the high losses that come without quantum repeaters.

To achieve global quantum connectivity, multi-segment entanglement distribution links will be required. While one satellite link might span 1000 km, the rate at which we can distribute entanglement will be too low for real-world applications. To overcome this will require both new space-based components such as quantum memories and repeaters as well as more complex satellite constellations.

Hybrid satellite-ground quantum repeater schemes have been proposed, such as that by Boone *et al.*[59], where entangled photon-pair sources are located on satellites. Ground stations are equipped with quantum non-demolition detectors and quantum memories, permitting entanglement creation at viable rates over distances inaccessible through optical fibers.

Networking

While we have already seen applications that will be enabled by quantum links alone, networks are much more than fixed links connecting specific locations for a single purpose. To realize novel applications, we will need to abstract away from the physical layer and enable seamless connectivity between devices across an entire network. Quantum networks may include trapped-ions, superconducting circuits, and solid-state systems which are not directly compatible with existing telecommunications networks. This will require interfacing and routing between the vast array of different systems being developed for quantum communication.

For quantum information processing at nodes, quantum states must be well preserved over physical distance and time. The information encoded in quantum states must arrive at the end-user with high fidelity. Quantum error correction, entanglement swapping, and quantum memories will contribute to the information being sent across a network and processed at nodes without errors or decoherence. Due to the weakly-interacting nature and long coherence times of photons, photonic qubits are well studied and frequently used for quantum communication protocols, but matter qubits are being considered for future network requirements such as quantum memories.

Quantum memories

For complex communication tasks, we will need to process information arriving from many different places. However, the information may not arrive simultaneously meaning we will need to store some information for a short time. Quantum communication will be no different, especially as loss along a channel may mean that the information does not arrive at all. In this instance, we will need ***quantum memories***[60] so that we can synchronize quantum information for processing. This will be especially important for quantum repeaters.

A quantum memory is a device that can store a photon without destroying the quantum information. The photon can then be recalled later when needed. One critical consideration with quantum memories will be the storage time, or *lifetime*. This is the length of time that a photon can be stored in a memory and be reliably recalled. As with single-photon sources, we are also concerned with the fidelity of the state recalled; any errors caused by a memory will propagate once the photon is recalled.

Many of the deterministic single-photon sources that we introduced in Chapter 4 are promising candidates being explored as quantum memories. Instead of stimulating the emission of a photon from an electron transition, a photon is absorbed by an electron and the quantum information transferred onto a property of the atomic system. Demonstrations of quantum memories include neutral atoms, trapped ions, color centers in diamond, solid-state spins, quantum dots, rare-earth-ion doped crystals, superconducting qubits, and various temperature atomic vapors. Each implementation has unique advantages to offer, but all currently have significant challenges to overcome before being widely deployed. The capability of storing quantum information will be vital in the development of quantum networks making quantum memories a critical roadblock to future developments.

Transducers

Given the variety of interacting quantum systems that will be used in quantum technologies of the future, especially quantum networks, it is imperative that seamless interfacing is carried out for reliable communication, computing, and sensing protocols. Quantum interconnects can occur between different quantum systems each with unique requirements.

The ability to reliably convert quantum information from one material system to another without loss of coherence is the purpose of ***quantum transducers***[61]. For example, information encoded in the polarization of a photon with a short wavelength may need to be converted to different encoding in a photon of telecom wavelength to be transmitted over fiber-optic channel with low loss. For this, we require a quantum transducer, and this optical conversion at scale is an ongoing research challenge.

Optical cavities are a popular choice for photonic interaction with matter-based quantum memories. One option for frequency conversion between photons stored in matter qubits and photons used for communication at various wavelengths requires a setup that features non-linear frequency conversion components such as non-linear crystal cavities. There is also research highlighting entanglement-based quantum transduction where photonic frequency conversion is carried out via teleportation of high-fidelity microwave-optical entangled states[62]. Additionally, rubidium atoms have been used to absorb microwave photons with quantum information, emitting optical photons with that same information due to the nature of transitions between energy levels of the atom[63]. There are many research investigations into multi-faceted quantum systems that exhibit similar photon emission properties. Regardless of the platform, quantum transducers will be required to interface various quantum systems for the operation of long-distance quantum networks.

Switches

Optical switches are used to actively route signals along selected pathways in all types of networks. Quantum optical switches enable entanglement distribution protocols as well as efficient node-to-node pathway choice and teleportation of information between end-users while maintaining quantum coherence. Unlike classical networks, where the flow of information from node to node is well defined, the quantum network allows for simultaneous traversal of the network where the order of paths taken cannot be determined. Researchers have shown that the use of the quantum switch produces a noiseless heralded quantum teleportation process with a probability that counterintuitively increases with the noise levels in the included pathway channels[64]. This is an ongoing research area where theoretical treatments and simulations of quantum switching aim to determine any advantage that these devices provide in multichannel networks. Results may lead to experimental implementations of quantum switches, bringing them closer to realization in a network.

Quantum network developments

Since the early 2000s, there have been many demonstrations of quantum networks around the world, the earliest of which was the DARPA quantum network[65] that was operational in 2003. In the following years, quantum networks have been deployed across North America, Europe, and Asia.

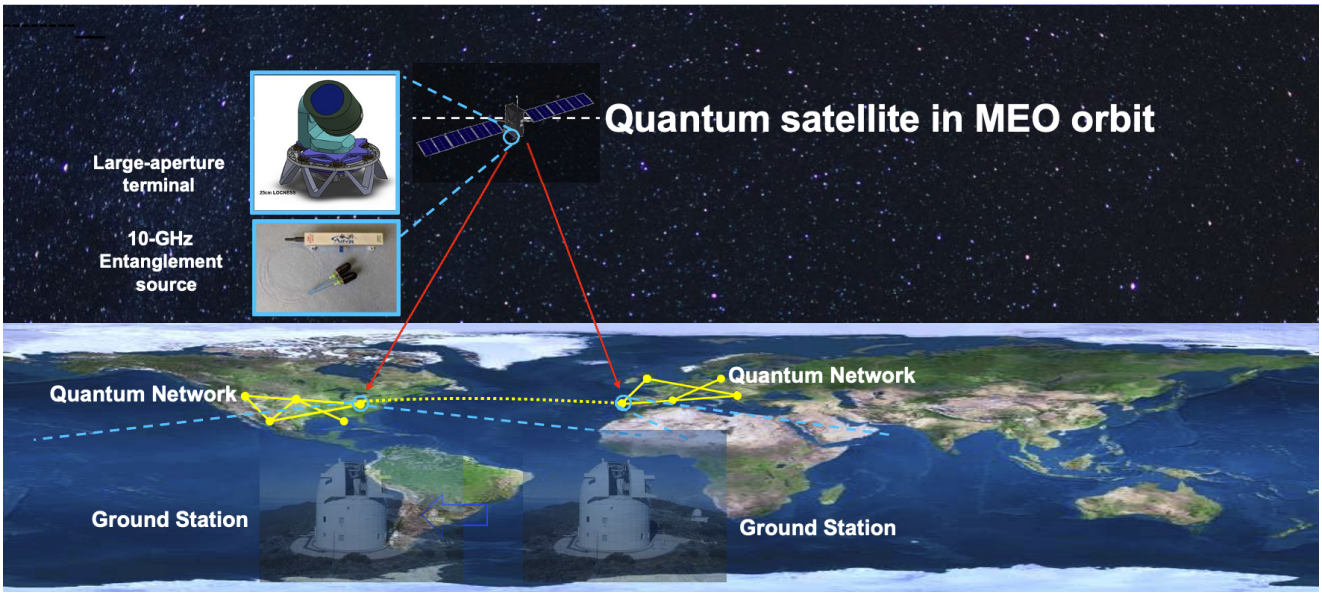


Figure 8.5: NASA's SCaN M2.0 mission concept to enable intercontinental quantum communication.

Several quantum networks are being developed across the US-based on fiber connectivity. Illinois-Express Quantum Network (IEQNET) comprises Fermilab, Argonne National Laboratory (ANL), Northwestern University, and the California Institute of Technology (Caltech), and this network recently achieved long-distance synchronization of quantum and classical signals sharing an optical fiber at 50 km[66]. The IEQNET also boasts active quantum networks supported by researchers at Caltech and Fermilab with exciting quantum teleportation results[67].

The Chicago Quantum Exchange (CQE) hosts quantum nodes at ANL, University of Illinois – Chicago, Chicago State University, and the University of Chicago with a fifth node at the CQE headquarters. Both Illinois based networks will have a multi-tiered approach to quantum communication, sponsored by industrial and US government collaborators.

Finally, a three-node network connects Brookhaven National Lab (BNL) and Stony Brook University (SBU), spanning 140 km. Built on current fiber-optic infrastructure, the two node stations, Alice and Bob, are located at SBU with the third node station, Charlie, located at BNL. There are plans for two more node stations for a total of five, expanding the current network to include Long Island to New York City. Free space optical links are also being developed for a fully entangled, quantum repeater-enhanced hybrid quantum network.

The atmospheric network constructed at the AFRL's Starfire Optical Range (SOR) has a connection between two ground stations, Alice and Bob, located one mile apart. Several tests of realistic, day-time atmospheric conditions have shown that atmospheric channels are feasible for quantum networks[68–70]. The SOR is leading the way in this effort, utilizing the corrective action of adaptive optics to counter atmospheric effects in free-space network channels[22,71,72].

NASA's SCaN quantum network mission concepts

Satellite networks carrying quantum processing payloads communicating with ground stations have many technical challenges but offer a promising route towards intercontinental quantum networks.

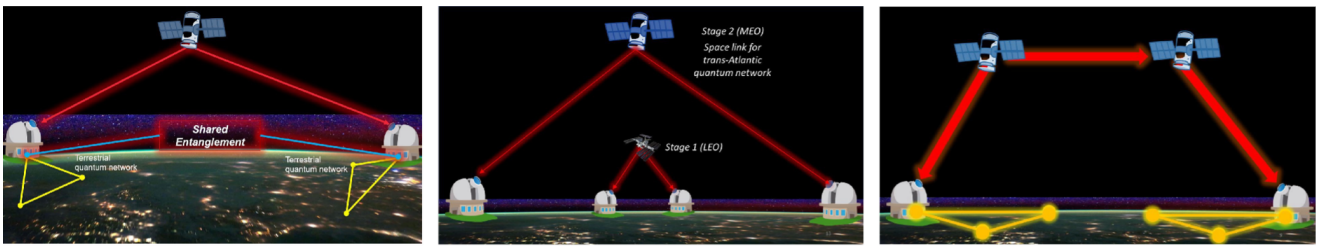


Figure 8.6: Example architectures for the three phases outlined by the qEDISON concept for space-based entanglement distribution.

NASA scientists and engineers are meeting this challenge with several mission concepts aiming to ultimately enable entanglement distribution between ground stations.

NASA's SCaN has proposed an LEO quantum testbed capable of linking ground stations separated by 100 km. This would utilize uplink-only connectivity to enable Bell state measurement in space along with SPDC entangled-photon sources.

The M2.0 mission concept seeks to expand on the LEO testbed to develop a unique platform and user facility to test quantum communication protocols and emerging quantum networking technologies. The concept is shown in Figure 8.5 and includes a quantum-capable satellite in MEO containing a source able to generate entangled photons at high rates (10 GHz). These entangled photons will then be distributed between intercontinental ground stations separated by thousands of kilometers, which may in future form part of larger quantum networks on the road to the advancement of a future global quantum internet. The ground stations will be equipped with adaptive optics and large telescopes and should be capable of high-fidelity reception of entangled photons, making possible both single- and dual-entanglement swapping.

The *Quantum Entanglement Distribution in Space Optical Network (qEDISON)* is a preliminary concept that aims to provide a source of quantum-entangled systems that can be used for teleportation, entanglement swapping, and ultimately quantum repeaters. This effort is in response to the multidisciplinary technological challenges of building full-scale quantum networks, while continually moving forward with current capabilities. The qEDISON concept is a multiyear, multiphase approach to the production and deployment of space-to-ground/space quantum links with readily available technology today, in anticipation of infrastructure that can be seamlessly integrated as future advancements come online such as quantum repeaters. At present, the MEO vehicle set to carry various quantum processing equipment is in development.

The qEDISON preliminary concept is separated into three phases, each with increasing technical capabilities, examples of which are shown in Figure 8.6. The aim of the first phase is to demonstrate entanglement swapping protocols between an LEO satellite and a ground station. The second phase will see the construction of the MEO spacecraft that will enable high-fidelity quantum processes across greater distances between ground stations. Finally, the project aims to demonstrate space-to-space quantum communication using current technology in a variety of LEO/MEO configurations.

Network type	Project operations	Maximum range between ground stations	Required technology development
Quantum fiber network	T + 1 year	200 km	None
Quantum fiber network++	T + 10 years	10 000 km	Quantum repeaters
qEDISON - Stage 1 (LEO)	T + 5 years	1200 km	Flight quantum subsystems; ground receivers
qEDISON - Stage 2 (MEO)	T + 7 years	5000 km	Flight quantum subsystems; ground receivers; large aperture flight terminals
qEDISON - Stage 3 (LEO-LEO crosslink)	T + 5 years	5000 km	Flight quantum subsystems; ground receivers
MEO Beacon with quantum memory	T + 10+ years	5000+ km	Flight quantum subsystems; ground receivers; large aperture flight terminals; flight quantum memories
GEO Beacon	T + 7 years	10 000 km	Flight quantum subsystems; ground receivers; large aperture flight terminals; flight quantum memories

Table 8.1: Alternative network protocols to qEDISON considered by NASA for quantum space-to-ground/space applications. Timelines are compared for each proposed method with required technological development[4].

In phase 1 of the qEDISON concept, entanglement distribution and swapping may alternatively be conducted between two space terminals, which may then in turn become part of two space-based quantum networks. Similarly, the technological developments in phase 1 also provide the opportunity to collaborate on unique scientific experiments and demonstrations with other global satellites such as QEYSSat[73] (Canada), SPooQy[74] (Singapore/UK), QUBE[75] (Germany), and QUARTZ[76] (Germany).

A variety of network platforms, shown in Table 8.1, have been considered by NASA. Each platform presents its own challenges, and it was concluded that the LEO spacecraft would reduce program risk and provide high-rate quantum communication resources for regional network applications[4]. The future of quantum networks, especially given the promise of the quantum internet, is exciting indeed. The framework of using current technologies, with capacity for expansion to advanced methods going forward, makes the qEDISON mission concept[4] being developed at NASA one to follow.

Building quantum networks requires an interdisciplinary team of scientists and engineers to overcome a wide range of challenges. As research is carried out, proof-of-concept designs demonstrated, and further progress made, new challenges continue to arise. These technical puzzles present a high barrier for quantum communication, but the technological promise and capability of quantum-enhanced communication protocols provides great motivation for overcoming these challenges.

9 The Quantum Internet

Having laid the foundation of quantum information and networks and explored some of the first applications of nascent quantum communication technology, we turn our attention to the future of quantum communication. As quantum communication technology develops, larger and more advanced quantum networks will be built with increasing functionality. Entanglement generation currently enables very small networks that stand as proof-of-concept demonstrations. As quantum memories mature, these networks will quickly grow across cities. Transducers will enable more devices to be connected and for quantum information to be transmitted across countries. Finally, by utilizing constellations of satellites and quantum repeaters, global connectivity becomes achievable. The culmination of this development, and the pinnacle of quantum communication, is the ***quantum internet*** – a network of networks seamlessly connecting quantum devices.

The quantum internet is a quantum information processing network built out of many smaller quantum networks. Quantum processing nodes are connected by quantum communication channels, with entanglement-based communication, and will enable applications beyond the capabilities of current technology. Throughout this booklet, we have introduced the necessary components and infrastructure from which the quantum internet will be built, some of which are summarized in Figure 9.1.

This chapter will introduce some of these emerging applications of the quantum internet in the fields of metrology, computing, and security. These serve as examples of the potential that the technology offers. However, as with any new technology, it is out of our grasp to truly predict quite how revolutionary the quantum internet might be with most applications yet to be discovered. As fundamental research flows through technology readiness levels, innovative frameworks, and system integration for quantum distributed computing and sensing will bring the realized quantum internet to the global stage.

Distributed quantum sensing

In Chapter 7, we introduced the field of metrology and how a probe system can be used to estimate a parameter of a physical system. In the classical case, the precision is fundamentally limited by the standard quantum limit. However, by introducing quantum states, we can go beyond this bound and perform more precise measurements.

As quantum sensing techniques improve, capabilities in measurement edge closer to the fundamental limit. Earlier in the booklet we considered using individual states, but in principle we could consider larger or entangled quantum systems as our probe. When using an entangled system, the individual noise factors are reduced in lieu of their collective quantum correlations, which results in an overall average noise factor lower than that of individual qubit noise contributions.

Distributed quantum sensing[77] looks beyond individual quantum states and explores how networks of entangled sensors can exhibit exponential measurement sensitivity and is one of the most exciting applications of quantum networking.

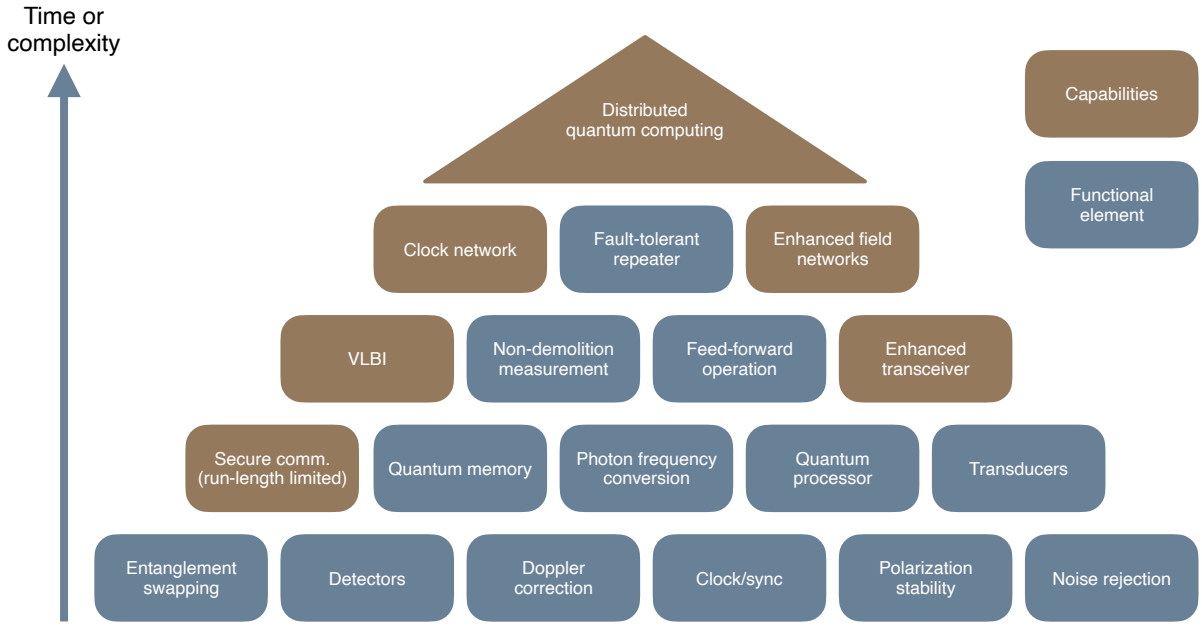


Figure 9.1: NASA functional elements and capabilities expected timeline chart for future quantum technologies, some of which have been introduced throughout this booklet. For a comprehensive review of these technologies, we refer the reader to the workshop report[4].

Very long baseline interferometry

Quantum metrology already plays a huge role in modern distributed sensing. Interferometry is the study of how waves interact constructively and destructively, and is used to make very precise measurements. To increase the precision of these measurements, the interferometer must be made very large. For example, each arm of LIGO spans 4 kilometers and achieves a measurement precision of 10^{-18} meters. However, there is a limit to how large we can feasibly make the paths in an interferometer. Instead, we can create an artificial interferometer with sensors distributed across the globe. This is the idea behind very long baseline interferometry which is a type of astronomical interferometry.

Around the world, we have many telescopes measuring radio waves emanating from our universe. The precision of each individual telescope is limited by the size of the antenna. To increase the precision, we can combine the data from many distant telescopes to create an *artificial* antenna. This requires the time of each measurement to be recorded with incredible accuracy. Each telescope uses an atomic clock to record the precise time that the signal arrives. The data from the network of telescopes is recorded and combined for analysis. As each telescope is a different distance from the source, we can combine the signal from each telescope, along with their locations, to reconstruct the interference just as with a standard interferometer. In April 2017, this technique was used to take the first picture of the event horizon of a supermassive black hole[78]. The complexity of the analysis and confirmation of the result meant that it took two years for the result to be published.

It has been proposed that instead of atomic clocks to synchronize each telescope, entangled states could be used where the quantum phase can be used as a reference. Such schemes could enable interferometric measurements in optical wavelengths where traditional methods are not sensitive

enough. Entangled photons could be distributed between satellites[79] but the performance might be limited by photon loss. This could be overcome by using a network of quantum repeaters to reliably distribute entanglement between telescopes[80], which would allow an artificial antenna array much larger than possible today.

As current entanglement distribution technology is limited, it is not clear to what extent quantum memories or repeaters will be required to improve the performance of very long baseline interferometry. One aim of the SCaN program is to determine whether quantum repeaters will be required to demonstrate a quantum advantage.

Clock synchronization

Beyond interferometry, clock synchronization is critical across modern communication and has enabled global navigation systems such as GPS, Galileo, and BeiDou. Impeccable timing resolution and synchronization is especially critical in space navigation to ensure mission success. Modern atomic clocks offer incredible performance but are not optimized for the low size, weight, and power requirements of spaceflight. There are many promising areas being explored to tackle this and make atomic timing more accessible.

As we saw above, entanglement can be used to synchronize distant devices and can also be used to create a quantum network of clocks[81]. Proposed quantum clock networks could enable time synchronization beyond the SQL (see Chapter 7) which would reduce the number of resources required. These protocols may also enable real-time synchronization, as opposed to the clock averaging that must be performed today, and eavesdropper detection to secure clock networks against tampering.

Satellite constellations of sensors using atomic clocks have a wide range of applications in imaging and can be used for gravimetry. Enhanced timing synchronization may allow for super-resolution imaging to reveal changes in local aquifer levels or map the sub-surface of the moon.

Future applications

Distributed quantum sensing is a broad field with proposed applications beyond astronomy and clock synchronization. Recently, machine learning has emerged as a promising new tool in tasks such as classification. With quantum sensors offering an advantage, it is natural to consider how machine learning could help us develop more optimal sensing schemes. Recent developments have explored a hybrid method to utilize both classical and quantum processing of entangled quantum sensor networks[82]. This work explores how a classical supervised-learning algorithm can be used to find an optimal quantum state shared between distributed sensors.

We may also find that distributed quantum sensors offer new techniques to measure properties of the universe not yet discovered. In the search for dark matter, several studies currently revolve around methods to detect a theoretical particle of unknown mass called an axion[83]. Distributed quantum states of light[84] (squeezed light that we introduced in Chapter 7) might serve as a probe with the precision necessary to shed light on this scientific mystery.

Demonstrations of quantum sensor networks remain elusive, and it is an open question whether distributed quantum sensing will provide an advantage over classical methods. Only once large, error-free quantum networks become available will we be able to test the applications and determine their real-world performance.

Distributed quantum computing

One of the most impactful applications of quantum information science is quantum computing, which promises to solve important problems in areas of chemistry, material science, simulations, optimization, and cybersecurity. Certain important problems that are intractable with classical computers will become solvable with quantum processors. Many approaches to quantum computing are being actively researched, each with their own challenges to overcome. However, it is widely anticipated that large-scale quantum computers will be realized in the coming years.

The main challenge shared between all approaches to quantum computing is scalability; how can we build a device with enough qubits to run quantum computing algorithms? Due to the complexity of the hardware required, building a single, large-scale quantum computer might not be possible. Instead, it has been proposed that smaller quantum devices with fewer qubits could be built and interconnected.

At first, this could help scale a single quantum computer by enabling short-range connectivity between processing units in a single system. For example, short-range microwaves can be used to interconnect superconducting processors housed in a single cryostat. As interconnects develop, separate quantum computing systems could be connected to form a cluster. We invite the reader to imagine a data center or computing cluster where quantum computers are housed in a single room and are connected to form a local network.

As the technology matures, truly remote devices and clusters could be connected in a quantum network that could be used as a single, large-scale quantum computer with capacity beyond each individual machine. At this stage the quantum computers are separated by greater distances, that will need more complex communication links and networks that will require the developments that we introduced in Chapter 8.

Collectively using quantum computing devices that are connected in a network is known as ***distributed quantum computing (DiQC)*** for which quantum communication is essential. The requirements for a network to connect distant quantum processors together will be very stringent and far beyond the capabilities of today. However, the current work will form a foundation to develop future networks.

An ambition as part of the SCaN program at NASA, is to include quantum processors onboard satellites as well as for them to serve as quantum repeaters enabled by entanglement distribution. These processors on orbiting satellites would serve as network nodes for several quantum technologies discussed in this chapter.

A quantum computer with distributed parts will have an architecture that is widely different from a single quantum processor system. A key challenge for distributed quantum computing is how we can

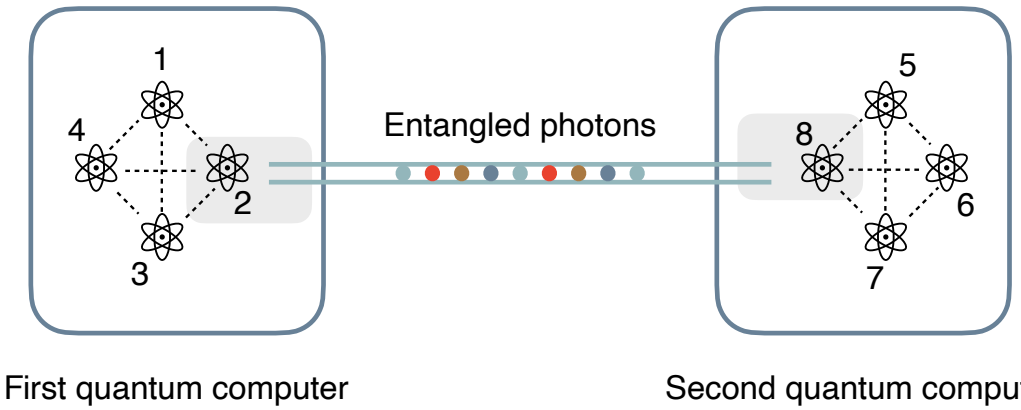


Figure 9.2: An illustration of two quantum computers interconnected using entangled photons, allowing for the combination of their computational power. Although the two individual computers have a fully connected architecture (all qubits can interact with any other), the resulting distributed resource is partially connected through qubits 2 and 8 only, which need to mediate the interactions between other remote qubit pairs. Additionally, the setup may require transducers (gray shaded area) to enable interactions between different physical qubit encodings.

divide an algorithm among the different connected processors. This is known as *quantum algorithm partitioning*. Qubits in a single device might have been able to connect with every other qubit in the device. In a distributed quantum processor, the qubits are part of a complex network with limited connectivity between groups of qubits. For example, Figure 9.2 shows two quantum processors connected via an entangled link between qubits 2 and 8. This makes the problem of compiling a quantum circuit and assigning qubits very complex as connectivity constrains and overheads must be considered.

A specific challenge is to reduce the communication time needed to establish quantum entanglement, to minimize the chance that quantum information is lost through decoherence. This problem is exacerbated as the communication qubits may require transducers to interact with computation qubits. If, for example, the communication qubits are infrared photons which are compatible with existing network infrastructure, they must be converted to visible wavelengths to interact with computation qubits encoded in ions.

Fundamental to quantum computation is the quantum circuit model of computation, in which input qubits go through a series of gates (or transformations) and are measured to provide an output. Some of these gates involve operations on multiple qubits, such as two-qubit controlled gates which perform a transformation on one qubit depending on the state of the other.

A major constraint for distributed quantum computing is performing quantum gates between qubit pairs located at remote processors. Consider, for example, qubits 1 and 7 in Figure 9.2 that are not directly connected. In this case, we can use a communication qubit to teleport one of the quantum states of interest from one device to the other to perform a two-qubit gate locally. Alternatively, we can also use this idea to perform *non-local* gates, in which the communication qubit is used to perform a gate on two qubits that remain on separated devices. This motivates developing quantum algorithms that can be easily partitioned where most gates on multiple qubits are performed only between qubits locally.

It has been shown that distributed quantum processors can implement any quantum circuit[85], but the network connectivity required is complex which makes implementation very challenging. Research-proposed solutions to partitioning algorithms often only apply for specific applications[86–88]. For those algorithms that can be partitioned, quantum information processing protocols such as those mentioned earlier in the booklet are viewed as compatible with the distributed quantum computing model.

Nevertheless, distributed quantum computing is foundational for several quantum network applications, including the quantum internet and distributed quantum sensing. The ability to construct quantum processing nodes at scale for both terrestrial and space networks will enable long distance communication of quantum information. There are several space-based programs that are planning for the day that distributed quantum computing is accomplished across larger networks.

Delegated quantum computing

Although its evolution is hard to predict, it is anticipated that quantum will follow the same path as classical computing. The first quantum computers already are, and in the near-term will continue to be, available only from a few providers with the expertise to build them. This implies that for most users, or clients, these will need to be accessed remotely. In a distant future, even if personal quantum computers may appear like personal classical laptops have, the most powerful quantum computers are likely to remain in the hands of service providers offering quantum compute time through remote access. This is analogous to today's cloud computing model, where clients can rent compute time on powerful computing clusters.

Computing on remote devices opens a range of security concerns. When the computation itself is sensitive information, it may be crucial to be able to hide the relevant information from the quantum computer provider. For example, when simulating the properties of a complex molecule for drug design, one might want to keep secret all information about the computation so that the computer provider cannot learn anything about it. One can encrypt the instructions to the quantum computer provider to keep it secret against third parties, but how can one keep information secret from the provider that needs to perform the computation? This task is called ***blind quantum computing (BQC)***.

Similarly, one might want to verify the computation, both to detect honest errors coming from implementation imperfections but also to check that the provider has indeed run the computation on a quantum computer as promised. Given the result of the computation, how does one check its correctness? It might be easy to check the result of prime factorization that we saw in Chapter 6, but how does one verify the result of the simulation of a complex molecule without the cost of producing it? This is known as ***verifiable quantum computing***. Verifiable and blind quantum computing are two aspects of the more general field of ***delegated quantum computing (DQC)***[89,90].

The role of quantum communication

For this discussion, we call the party who wishes to perform the computation the *client* and the party who will perform the computation on a quantum computer the *server*. To instruct the computation on

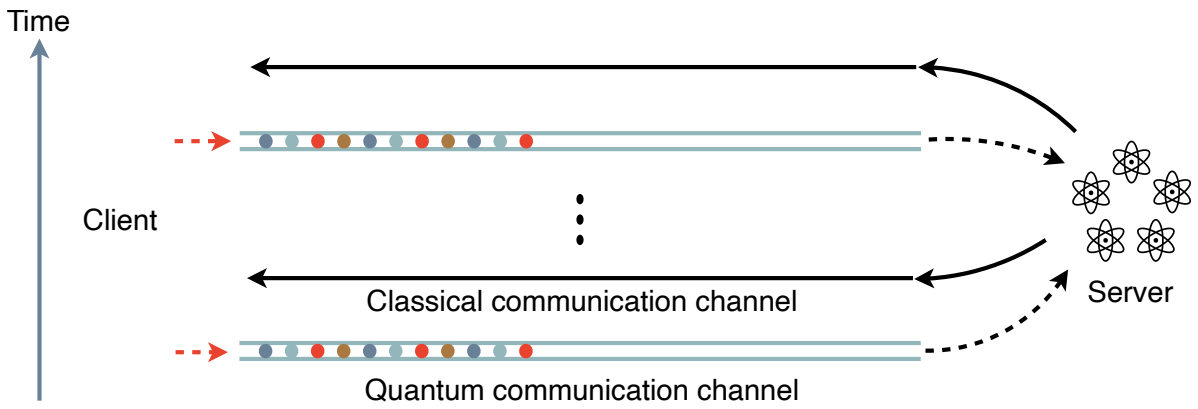


Figure 9.3: A delegation of a quantum computation from a client with minimal quantum capabilities to a server owning a quantum computer. The delegation is made of multiple rounds of interactions, in which the client prepares simple quantum systems which are transmitted to the server over a quantum channel.

the remote device of the server, the client needs to send it the relevant information: the computation (or program) that needs to be performed and its input. Using our example above, one could send the instructions to simulate a molecule for drug discovery and the description of the molecule. After computation, the server returns the output of the computation to the client which, in this example, is the molecule simulation. As the server is remote, delegated computing fundamentally relies on communication.

The simplest method to delegate a computation is to send the full details of the computation and its input to the server and ask the server to complete the computation and return the result. In this case, the server has access to all information and may learn the method to simulate the molecule and its behavior, which we would have liked to keep secret. Therefore, to perform blind quantum computation we will need to develop a more complex protocol.

One method to perform blind quantum computation relies on the existence of one-way functions, that we discussed in Chapter 6, which introduce computational assumptions on security[91,92]. Instead, we will focus on two methods which harness the strengths of quantum communication to perform our calculation.

An illustration of an interactive delegated computation is provided in Figure 9.3. The first method to perform our computation relies on the client having the capability to prepare or measure very simple quantum states and, crucially, a quantum communication link with the server. By preparing quantum systems in a state unknown to the server, the client hides the relevant information to the server in a way similar to QKD (see Chapter 6). This procedure is *interactive*; upon receiving the quantum systems from the client, together with instructions, the server performs complicated quantum operations on the systems that the client is unable to perform themselves. The server then returns some intermediary results to the client who, based on said results sends additional quantum systems and instructions to the server. These steps are repeated until the desired computation has been performed. Based on the same ideas as QKD, it is possible to hide both the input and details of the computation to the server, which is also unable to interpret the obtained results.

In this approach, the client also adds trap systems, which serve for *verification* of the computation[93,94]. These traps are put in a state for which the client knows the result of the computation it requests from the server, whilst the server does not. In this way, the client can check that the trap results correspond to the expected ones, both detecting cheating strategies by the server and honest errors coming from unavoidable implementation noise.

Using this method to perform both blind and verifiable quantum computing, the objective is then to minimize the necessary quantum resources of the client, the number of interaction rounds, the number of qubits that need sending, and the complexity of the computation that needs to be performed by the server. Note that because we require the computation to be blind and verifiable, there is an overhead when compared to running the original computation directly on the quantum computer. Results have shown that it is possible to do blind quantum computation with a client preparing[93] or measuring qubit states[95] only, which is the minimal resource that one could hope for. On the other hand, having to send quantum states to the server once again highlights one of the main challenges of quantum information science and the central topic of this booklet: reliable quantum communication systems.

Due to losses in quantum communication channels, the benefit of using entangled systems shared between the client and server has been shown[93]. The client, by measuring one of the two systems in an entangled state, effectively remotely prepares the state of the second system on the server's side. As this process can be repeated until success, it eliminates the problem of channel losses.

The second method to perform blind quantum computation allows a client with only classical capabilities to instruct two servers to perform the desired computation on their respective quantum computers. This method relies on the two servers sharing entanglement. By instructing the first server to measure its entangled system, the client remotely prepares the state of the system received by the second server. Unlike the first method where the client prepares the state, this method employs one of the servers for remote state preparation. Importantly, this method relies on the first server not communicating the state preparation information to the second server, as then the second server would obtain all information about the computation. This may be hard to enforce in practice.

Interestingly, when relying on entanglement, both methods for blind and verifiable quantum computing can also be performed in a device-independent manner[96–98], like the case of QKD explained in Chapter 6. This allows for a much higher level of confidence and security, which is then independent from unavoidable implementation imperfections.

Recent developments

Several delegated quantum computations have already been demonstrated utilizing quantum optics. With the client sending photons to the server, both the Deutsch–Josza[99] and Grover's search algorithm[100] have been implemented as well as other blind operations on one and two qubit systems[101]. We note that only a subset of the information was kept hidden and not the whole computation, input, and output, but these demonstrate the possibility of delegated quantum computing. Similar protocols in which the client only measures systems sent by the server have also been demonstrated[95] and one in which the client only prepares quantum systems[102].

Beyond blind and verifiable computation

We note that blind and verifiable quantum computing only scratch the surface of delegated quantum computing. A related task, called *homomorphic encryption*, allows computation over data in an encrypted form, hence preserving secrecy. The advantage of homomorphic encryption over blind computation as we described is that it does not require interaction rounds between the client and server, drastically reducing that overhead. On the other hand, homomorphic encryption does not keep the computation to be performed on the data secret (only the data is), so may not be suitable for all scenarios. We also note that, although quantum cryptography can often avoid the reliance upon computational assumptions, this does not seem to be the case for homomorphic encryption[103] and computational assumptions will always be required even with quantum communication.

Quantum cryptography

In Chapter 6, we introduced quantum key distribution protocols which are possible to implement with current quantum communication technologies. Future quantum networks based on entanglement technology will offer the ideal support for mature QKD capabilities. The ability of a network to establish and route entanglement using repeater technology will enable QKD beyond dedicated point-to-point links. Entanglement will also enable new functionality for cryptography including device-independent protocols. Finally, although recent QKD systems, such as twin-field QKD, have demonstrated record breaking distances, the achievable distance is still fundamentally limited without mature quantum repeater technology.

However, quantum cryptography will greatly benefit from the development of the advanced components and functionalities for quantum communication, even before the advent of a fully functional quantum internet. Beyond futuristic QKD systems, advanced quantum networks are expected to enable new applications in the field of quantum cryptography. We have already discussed the security aspects of delegated, blind, and verified quantum computing earlier in this chapter.

The field of quantum cryptography is incredibly broad with intricacies that are beyond the scope of this booklet. However, we will briefly introduce some of the emerging applications for future quantum networks and equip the reader with necessary terminology so that they may research the topic further.

Quantum money[104] is seminal to quantum cryptography, as it was the first invention making the link between the properties of quantum mechanics and applications in cryptography. The task is the creation of quantum versions of money and tokens. Central to the concept of money is *unforgeability*: the inability to make copies of a banknote, for example. The attraction of using the no-cloning principle of quantum states is that is can be harnessed to build quantum money that is unforgeable. Like banknotes, quantum money can be used near-instantly (its validity can be verified on the spot), but unlike banknotes it is physically impossible to forge. More generally, the subfield of quantum cryptography called *unclonable cryptography* studies the new possibilities specifically offered by the no-cloning principle. To implement such schemes, one will require future quantum technology such as quantum memories.

Quantum digital signatures[105] are an alternative to public-key authentication presented in Chapter 6 that replace classical keys (bitstrings) by quantum states that play the new role of public keys.

Other examples include quantum cryptography with certified deletion[106,107], in which the receiver can provide a certificate that the received quantum information (in particular an encrypted message) has been destroyed, hence making future attacks on it impossible. Network tasks such as quantum conference (or group) key agreement[108] and secret sharing[109] might also offer a quantum advantage. Secret sharing allows multiple players to share a secret (for example a cryptographic key) together, while requiring that a given minimum number of players need to share their information to recover the secret. This is particularly useful to store sensitive information across multiple places, making it resilient to the failure, leak, or attack of a subset of these. Classical secret sharing schemes are often used in cloud environments with multiple servers. Conference key agreement is a generalization of key distribution to more than two parties, where the goal is to establish a secret key within the members of a group only.

Finally, quantum protocols for quantum byzantine agreement[110], oblivious transfer[111], and coin flipping[34] have also been proposed. Byzantine agreement allows building protocols that are immune to faulty (or even malicious) parts of a distributed system, whereas oblivious transfer allows a sender to transfer one of many pieces of information to a receiver whilst remaining oblivious to which part was transmitted. Oblivious transfer is a fundamentally important task in cryptography and is the foundation for secure multiparty computation. Coin flipping allows two parties who don't trust each other to agree on a random bit (or coin flip), which can also be used to construct more complex protocols.

One of the most appealing aspects of quantum cryptography is that we can develop protocols where the security does not rely on hardness assumptions of a mathematical problem. The security of many of the applications described above instead stems from properties of quantum physics. Given the importance of cryptography in communication, quantum cryptography is a strong motivator for the development of quantum networks.

10 Summary and Open Problems

Quantum technologies are set to revolutionize the field of information science and epitomize the continuation of the digital revolution which began in the last century. After having led to technologies such as the laser, MRI, and nuclear energy, our ability to control individual quantum systems opens a new range of applications across computing, sensing, and cryptography.

Quantum communication stands as a core pillar in this quantum age. As quantum technology continues to develop, we will soon be able to build long-distance quantum communication links and quantum networks with increased communication capabilities, eventually leading to the quantum internet. Quantum computers will be interconnected to increase their computational power, eventually surpassing the most powerful supercomputers at certain tasks. They will become widely accessible remotely by clients who wish to keep sensitive information secret. Distributed quantum sensors based on unique quantum effects will obtain sensitivity that is not possible to achieve classically. Finally, important enhancements in the way that we secure information will also be obtained.

Even before a mature quantum internet exists, the development path promises many near-term applications, making both the journey and the end goal worth the investment. Today, the first quantum links are being used to demonstrate quantum applications in cybersecurity and metrology. Quantum key distribution is being used to establish keys for secure communication and extremely sensitive interferometers are providing valuable insights into our universe through measurements of gravitational waves.

Central to the transmission of quantum information over large distances is the generation and distribution of entanglement – a unique quantum property with no classical analogue. Through entanglement distribution we can hope to build quantum repeaters to overcome the impossibility of amplifying quantum signals for long-distance quantum communication. Additionally, entanglement will provide quantum-enhanced security through device-independent protocols and precision measurements which surpass our most advanced metrological capabilities to date. Satellite constellations of sensors using atomic clocks which are entangled could allow for super-resolution imaging and distributed quantum light might provide answers in the ongoing search for elusive dark matter.

NASA's SCaN quantum communication roadmap will play a crucial role in this development, by enabling long-distance entanglement distribution using satellites. Both the M2.0 and qEDISON mission concepts aim to develop space-to-ground and inter-satellite quantum links with readily available technology. In the future, the hope is that these links will seamlessly integrate with quantum communication technologies such as quantum repeaters. These advanced quantum communication capabilities could serve as an ideal testbed for novel quantum applications through NASA's internationally collaborative effort.

In building long-distance quantum links and the first quantum networks we will face many challenges. Quantum components to prepare, manipulate, store, and measure quantum information will need huge technological advances to accurately and precisely control quantum particles such as photons and electrons. Shorter quantum communication links may be established with fiber-optic cables to build small or local quantum networks. Longer links and larger networks will be enabled by

Functional element	Year ready
Entanglement swapping between moving sources	2025
Feed-forward operation on teleported qubit	2025
High-efficiency, low-jitter photon detectors in space	2025
High-resolution clock and sync	2025
Single-photon frequency and bandwidth conversion	2025
Quantum memory	2030
Quantum transducer	2025-2030
Fault-tolerant quantum repeater	2035
Full-scale, error-corrected quantum processor	2030-2040

Table 10.1: Estimated timeline for several quantum technology functional elements adapted from the Workshop on Space Quantum Communications and Networks hosted by NASA in 2020[4]. The estimates here remain valid at time of writing.

quantum-capable satellites, making them an essential development for the quantum internet. There are many open questions and challenges that arise in the building of global and satellite-based quantum networks. Navigating free-space atmospheric turbulence for Earth-to-satellite links, fiber-optic attenuation at scale, and satellites moving relative to Earth is no easy task. Extensive research is underway to overcome these challenges; with NASA's development of technologies such as ultra-low-loss fiber, adaptive optics for satellite communication, and superconducting single-photon detectors in ground stations, we are edging ever closer to realizing quantum communication on a global scale.

Beyond Earth, connecting quantum devices at nodes located on moving spacecraft necessitates the study of general relativity, gravitational, and quantum effects in tandem on orbiting satellites and the quantum devices they will carry. This is the central aim of NASA JPL space-based quantum networking concept, the Deep Space Quantum Link (DSQL), which seeks to explore the relativistic effects on experiments involving teleportation and entanglement distribution[112].

Throughout this booklet, we have highlighted many challenges for the development of quantum communication: from components to abstract communication capabilities such as quantum repeaters and memories. All these challenges are at the core of NASA's SCaN roadmap. The timeline to achieving many of these essential building blocks, most of which were introduced throughout this booklet, is summarized by NASA in Table 10.1. Finally, NASA anticipates a demonstration of quantum communication at intercontinental distances by 2030.

In 1966, the Advanced Research Project Agency Network (ARPANET) was initiated with the aim of sharing resources between remote computers, taking three years for the first connections to be made.

At the time, no one could have predicted how this initial development would lead to the Internet and to what extent it would impact our global society. We now stand at the precipice of a new quantum revolution, at a time where nations across the globe have initiatives to develop quantum networks. The list of applications that will be enabled by quantum technologies is continually expanding and may impact our lives in ways we can not predict. Only once we reach the point of ubiquitous quantum communication, that lets us abstract away from the physical layer, will the most exciting applications reveal themselves. NASA's SCaN program lays out a path to achieve this.

Further Reading

NASA SCaN

NASA Space Communications and Navigation (SCaN) https://www.nasa.gov/directorates/space-operations/space-communications-and-navigation-scan-program/.

NASA SCaN, *Workshop on Space Quantum Communications and Networks*, https://www.nasa.gov/centers-and-facilities/johnson/workshop-on-space-quantum-communications-and-networks-proceedings/, (Sept. 2020).

Quantum communication

M. Hajdušek and R. Van Meter, "Quantum Communications", arXiv:2311.02367 (2023). Based on Q-Leap Edu Quantum Communications video tutorials: https://www.youtube.com/playlist?list=PLCTGenrx1-SOC-b98RCC1uEGI-Sc-N3C-.

K. Azume *et al.*, "Quantum repeaters: From quantum networks to the quantum internet", Rev. Mod. Phys. **95**, 045006 (2023).

Quantum information and computation

D. J. Griffiths and D. F. Schroeter, *Introduction to quantum mechanics* (Cambridge University Press, Aug. 2018).

M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information: 10th anniversary edition* (Cambridge University Press, Jun. 2012).

T. Wong, *Introduction to classical and quantum computing* (Rooted Groove, Jan. 2022).

Quantum light and metrology

R. Loudon, *The Quantum Theory of Light, Third Edition* (Oxford University Press, Nov. 2000).

C. Gerry and P. Knight, *Introductory Quantum Optics* (Cambridge University Press, Nov. 2004).

M. Fox, *Quantum Optics: An Introduction* (Oxford University Press, Jun. 2006).

Abbreviations

AES	Advanced Encryption Standard
AFRL	Air Force Research Laboratory
ANL	Argonne National Laboratory
AO	Adaptive optics
APD	Avalanche photodiode
ARPANET	Advanced Research Project Agency Network
BNL	Brookhaven National Lab
BQC	Blind quantum computing
Caltech	California Institute of Technology
CQE	Chicago Quantum Exchange
CRB	Cramér-Rao bound
DARPA	Defense Advanced Research Projects Agency
dB	Decibel
DI	Device-independent
DiQC	Distributed quantum computing
DoD	Department of Defense
DoE	Department of Energy
DQC	Delegated quantum computing
DSOC	Deep Space Optical Communication
DSQL	Deep Space Quantum Link
ESA	European Space Agency
FI	Fisher information
GEO	Geosynchronous orbit
GPS	Global Positioning System
GSFC	Goddard Space Flight Center
IEQNET	Illinois-Express Quantum Network
ISS	International Space Station
JPL	Jet Propulsion Laboratory
LCRD	Laser Communications Relay Demonstration
LEO	Low-Earth orbit
LIGO	Laser Interferometer Gravitational-Wave Observatory
MCP-PMT	Microchannel plate PMT
MDI QKD	Measurement-device-independent QKD
MEO	Medium-Earth orbit
MIT	Massachusetts Institute of Technology

MOT	Magneto-optical trap
MRI	Magnetic resonance imaging
MZI	Mach-Zehnder interferometer
NASA	National Aeronautics and Space Administration
NEN	Near-Earth network
NIST	The National Institute of Standards and Technologies
NQI	National Quantum Initiative
NSF	National Science Foundation
PAT	Pointing, acquisition, and tracking
PEACOQ	Performance-Enhanced Array for Counting Optical Quanta
PMT	Photomultiplier tube
PQC	Post-quantum cryptography
QCRB	Quantum Cramér-Rao bound
qEDISON	Quantum Entanglement Distribution in Space Optical Network
QFI	Quantum Fisher information
QIS	Quantum information science
QKD	Quantum key distribution
QME	Quantum multi-parameter estimation
QPE	Quantum parameter estimation
qubit	Quantum bit
RSA	Rivest–Shamir–Adleman
SBU	Stony Brook University
SCaN	Space Communications and Navigation
SFWM	Spontaneous four-wave mixing
SNSPD	Superconducting nanowire single-photon detector
SOR	Starfire Optical Range
SPAD	Single-photon avalanche diode
SPDC	Spontaneous parametric down-conversion
SQL	Standard quantum limit
TF QKD	Twin-field QKD
UAV	Unmanned aerial vehicle
VQC	Verifiable quantum computing

Glossary

Attenuation The proportion of signal lost during transmission, measured in units of decibel (dB).

Bell state measurement A joint quantum measurement of two qubits to determine which of the four possible Bell states the qubits are in. It can be used to generate an entangled state and is an important step in quantum teleportation.

Bit From *binary digit*, the most basic unit of information in digital computing and communication, most commonly represented as either '0' or '1'.

Bloch sphere The sphere of unit radius commonly used to visualize quantum states and transformations. The coefficients α and β in the qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ are explicitly connected to the angles of the Bloch sphere θ and ϕ. For example, if $\theta = 0°$, $\alpha = 1$ and $\beta = 0$, resulting in $|\psi\rangle = |0\rangle$, then the state is represented at the North pole on the Bloch sphere, while $|1\rangle$ is diametrically opposite to it.

Bunched light Chaotic light in which photons are emitted closer together (in bunches) than they would be if they obeyed Poissonian statistics. Light with a second-order correlation function $g^{(2)} > 1$ is described as bunched.

Coherent light Light with a constant phase relationship. For light from a laser, we find that the second-order correlation function $g^{(2)} = 1$, which is the condition for light to be coherent.

Cramér-Rao bound A lower bound on the variance of an unbiased estimator, which represents the limit in precision for measurements in classical estimation theory. In quantum parameter estimation, the *quantum* Cramér-Rao bound is the fundamental limit in precision measurement.

Cryptographically-relevant quantum computer A quantum computer that is powerful enough to run algorithms, such as Shor's and Grover's, that will compromise modern cryptography.

Decoherence The loss of quantum coherence, whereby a system's behavior changes from a quantum to a purely classical description, losing quantum information. Channel errors contribute to the decoherence of quantum signals.

Device-independence Describes systems in quantum cryptography which do not rely on a precise description or model of the hardware. Instead, all quantum parts of the system are seen as black boxes whose internal functioning is untrusted, leading to very strong promises for security.

Distributed quantum computing Using quantum computers that are separated but connected by a network to perform a single algorithm or computation. This will become relevant when quantum networks become more prevalent.

Entanglement swapping	A mechanism for distributing entanglement between distant systems that have not interacted. Alice and Bob have an entangled state each and send one particle from each state to a Bell state measurement device which entangles them. Measurement on these particles results in an entangled state shared between Alice and Bob.
Fisher information	Describes how much information about a parameter can be obtained from a sample measurement. The *quantum* Fisher information bounds the achievable precision in parameter estimation with a quantum system.
Grover's algorithm	A quantum algorithm for searching an unstructured database which is faster than the best-known classical algorithm. When searching a database with N elements, Grover's algorithm only requires $O(\sqrt{N})$ evaluations.
Heisenberg's uncertainty principle	States that there is a fundamental limit to the precision with which one can measure certain pairs of physical properties simultaneously. More precisely, for properties that are said to be complementary, the more accurately one property is measured the less accurately the other can be known. Mathematically, denoting the position of a particle with x and its momentum with p, it takes the form $\Delta x \Delta p \geq \hbar/2$, where Δ denotes the uncertainty of the given property to be measured. The reduced Planck constant $\hbar$ is a fundamental value limiting the joint precision that can be obtained.
No-cloning theorem	A fundamental result in quantum theory which states that it is impossible to make a copy of an unknown quantum state. This leads to the impossibility to amplify quantum signals, making long distance transmission of quantum information difficult, but has positive consequences in the field of quantum cryptography where eavesdroppers are detected on quantum channels.
Polarization	When considering light as an oscillating electromagnetic wave, its polarization is defined as the direction in which the electric field oscillates. For example, if the electric field oscillates along the vertical direction perpendicular to the propagation direction, that wave is linearly polarized along the vertical direction. Diagonally polarized light is a superposition of horizontally and vertically polarized light waves that are *in phase*.
Post-quantum cryptography	The science of developing classical cryptographic algorithms and systems which are secure against both quantum and classical computers.

Public-key cryptography	Cryptographic algorithms that are asymmetric where the key to encrypt is public, while the key to decrypt is kept private. These algorithms are typically used for key establishment or digital signatures.
Quantum advantage	A quantum computing milestone at which a quantum computer can solve computational problems that are beyond the reach of the most powerful classical computers.
Quantum entanglement	A uniquely quantum phenomenon in which multiple quantum particles exhibit correlations that do not respect their location.
Quantum internet	The quantum internet is viewed by many as the end goal of quantum communication and is characterized by our ability to seamlessly distribute quantum information across many individual quantum networks for sensing, processing, and securing data across the globe.
Quantum key distribution	A secure communication method for establishing shared randomness (a cryptographic key) between distant parties using quantum states.
Quantum links	Quantum links are optical channels through which we can send and receive quantum signals carrying quantum information for the purposes of quantum communication. They can be free-space, such as satellite-ground links, or optical fiber.
Quantum measurement	The process of reading a particular property of a quantum system to retrieve the information encoded in it. Although the value of a qubit was undetermined before the measurement, the qubit is *projected* to a determined value after a measurement. This mapping between a qubit state and a classical bit is therefore intrinsically probabilistic, which is unlike classical physics.
Quantum memory	Devices which can store a quantum state for some time without destroying the quantum information. Quantum Memories are essential for the development of quantum repeaters and long-distance quantum communication.
Quantum repeater	Quantum repeaters allow long-distance quantum links to be broken down into smaller sections to overcome channel losses. They are enabled by entanglement, which is shared between adjacent nodes before entanglement swapping is performed.

Quantum superposition A uniquely quantum phenomenon in which a qubit can correspond to a linear combination of 0 *and* 1, as opposed to holding a definite value of 0 *or* 1. While in superposition, qubits can represent many possible values simultaneously. However, only when an observation, or measurement, is made to read the state do we get a specific value. Before the measurement, it is not possible to say which value will be obtained from the qubits. In other words, quantum physics can be fundamentally unpredictable.

Quantum teleportation The transfer of a quantum state between remote systems that have not previously interacted by using shared entanglement and a Bell state measurement.

Quantum transducer Quantum transducers convert quantum information from one physical quantum system to another. For example, converting quantum information in an electron spin to an optical photon.

Qubit The quantum bit, or qubit, is the basic unit of quantum information and counterpart to the bit in classical information. Unlike bits, qubits can exist in a quantum superposition state where the state is not definitely $|0\rangle$ or $|1\rangle$ but instead must be described by a combination of the two. To write the state of a qubit in superposition, we use the sum $\alpha\,|0\rangle + \beta\,|1\rangle$ where α and β are numbers that describe the specific composition which, in general, are complex numbers.

Shor's algorithm A quantum algorithm that can efficiently find the prime factors of large numbers. This is relevant for public-key cryptography where the security relies on factoring being a difficult problem.

Squeezed state As a consequence of Heisenberg's uncertainty principle, when the uncertainty in one property of a quantum state is increased, the uncertainty in the complementary property is decreased, or squeezed, such that the principle is not violated. Squeezed states are used for increasing the precision of measurements past the standard quantum limit in quantum metrology.

Standard quantum limit The precision limit of measurement when only considering individual optical resources, as opposed to entangled resources. Where N resources are used, the measurement precision scales like $1/\sqrt{N}$.

References

[1]The Nobel Foundation, *The Nobel Prize in Physics 2022*, (2022) https://www.nobelprize.org/prizes/physics/2022/press-release/.

[2]E. Schrödinger, "Discussion of probability relations between separated systems", Mathematical Proceedings of the Cambridge Philosophical Society **31**, 555 (1935).

[3]D. Ganapathy et al. (LIGO O4 Detector Collaboration), "Broadband quantum enhancement of the ligo detectors with frequency-dependent squeezing", Phys. Rev. X **13**, 041021 (2023).

[4]NASA SCaN, *Workshop on Space Quantum Communications and Networks*, (Sept. 2020) https://www.nasa.gov/centers-and-facilities/johnson/workshop-on-space-quantum-communications-and-networks-proceedings/.

[5]J. S. Bell, "Bertlmann's socks and the nature of reality", Le Journal de Physique Colloques **42**, C2–41–C2 (1981).

[6]J. S. Bell, "On the Einstein Podolsky Rosen paradox", Physics Physique Fizika **1**, 195 (1964).

[7]A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via Bell's theorem", Phys. Rev. Lett. **47**, 460 (1981).

[8]P. Dhara et al., "Heralded multiplexed high-efficiency cascaded source of dual-rail entangled photon pairs using spontaneous parametric down-conversion", Phys. Rev. Appl. **17**, 034071 (2022).

[9]I. Aharonovich, D. Englund, and M. Toth, "Solid-state single-photon emitters", Nature Photonics **10**, 631 (2016).

[10]W. B. Gao et al., "Observation of entanglement between a quantum dot spin and a single photon", Nature **491**, 426 (2012).

[11]Y. C. Tan et al., "Silicon avalanche photodiode operation and lifetime analysis for small satellites", Opt. Express **21**, 16946 (2013).

[12]I. Craiciu et al., "High-speed detection of 1550 nm single photons with superconducting nanowire detectors", Optica **10**, 183 (2023).

[13]Chicago Quantum Exchange, *Chicago expands and activates quantum network, taking steps toward a secure quantum internet*, (June 2022) https://chicagoquantum.org/news/chicago-expands-and-activates-quantum-network-taking-steps-toward-secure-quantum-internet.

[14]Brookhaven National Laboratory, *BNL | Quantum Network Facility | Ongoing Research and Planned Expansion*, https://www.bnl.gov/instrumentation/quantum/research.php.

[15]EPB Quantum Network, *EPB Quantum Network | About Us*, (Nov. 2022) https://quantum.epb.com/about-us/.

[16]T. Miya et al., "Ultimate low-loss single-mode fibre at 1.55 µm", Electronics Letters **15**, 106 (1979).

[17]H. Kanamori et al., "Transmission characteristics and reliability of pure-silica-core single-mode fibers", Journal of Lightwave Technology **4**, 1144 (1986).

[18]Y. Tamura et al., “The First 0.14-dB/km Loss Optical Fiber and its Impact on Submarine Transmission”, Journal of Lightwave Technology **36**, 44 (2018).

[19]G. Workman, G. Smith, and D. Tucker, “Study of the effect of gravity on zblan glass as a commercial program”, in 36th aiaa aerospace sciences meeting and exhibit (Jan. 1998).

[20]G. L. Workman et al., *ZBLAN Microgravity Study*, tech. rep. NASA-CR-202759 (NASA, Apr. 1995).

[21]I. Cozmuta and D. J. Rasky, “Exotic Optical Fibers and Glasses: Innovative Material Processing Opportunities in Earth’s Orbit”, New Space **5**, 121 (2017).

[22]M. T. Gruneisen et al., “Adaptive-Optics-Enabled Quantum Communication: A Technique for Daytime Space-To-Earth Links”, Physical Review Applied **16**, 014067 (2021).

[23]J. C. Chapman and N. A. Peters, “Paving the Way for Satellite Quantum Communications”, Physics **15**, 172 (2022).

[24]C. Simmons et al., “An investigation of jamming in free-space quantum key distribution”, Proc. SPIE Int. Soc. Opt. Eng. **12335**, 84 (2023).

[25]R. K. Tyson and B. W. Frazier, *Principles of adaptive optics* (CRC Press, Jan. 2022).

[26]G. C. Loney, “Design of a high-bandwidth steering mirror for space-based optical communications”, in Active and adaptive optical components (Jan. 1992).

[27]B. M. Levine et al., “Horizontal line-of-sight turbulence over near-ground paths and implications for adaptive optics corrections in laser communications”, Applied Optics **37**, 4553 (1998).

[28]N. Johnson, “Medium Earth Orbits: Is There a Need for a Third Protected Region?”, in 61st International Astronautical Congress, IAC-10-A6.4.1 (Sept. 2010).

[29]S. Pirandola, “Satellite quantum communications: Fundamental bounds and practical security”, Physical Review Research **3**, 023130 (2021).

[30]NASA, *Laser Communications Relay Demonstration (LCRD) Overview*, (Dec. 2021) https://www.nasa.gov/directorates/stmd/tech-demo-missions-program/laser-communications-relay-demonstration-lcrd-overview/.

[31]M. Mohageg et al., “The deep space quantum link: prospective fundamental physics experiments using long-baseline quantum optics”, EPJ Quantum Technology **9**, 1 (2022).

[32]J. F. Spann, “Science and Exploration Deep Space Gateway Workshop”, in NASA Exploration Science Forum (NESF) (July 2017).

[33]P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM Journal on Computing **26**, 1484 (1997).

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

[35]The National Cyber Security Centre (NCSC), *Quantum security technologies*, (Mar. 2020) https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.

[36]National Security Agency/Central Security Service, *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*, https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[37]D. P. Nadlinger et al., "Experimental quantum key distribution certified by Bell's theorem", Nature **607**, 682 (2022).

[38]J.-P. Chen et al., "Quantum Key Distribution over 658 km Fiber with Distributed Vibration Sensing", Physical Review Letters **128**, 180502 (2022).

[39]S. Wang et al., "Twin-field quantum key distribution over 830-km fibre", Nature Photonics **16**, 154 (2022).

[40]J.-P. Chen et al., "Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans", Nature Photonics **15**, 570 (2021).

[41]H.-L. Yin et al., "Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber", Physical Review Letters **117**, 190501 (2016).

[42]S.-K. Liao et al., "Satellite-to-ground quantum key distribution", Nature **549**, 43 (2017).

[43]J. Yin et al., "Satellite-based entanglement distribution over 1200 kilometers", Science **356**, 1140 (2017).

[44]S.-K. Liao et al., "Satellite-Relayed Intercontinental Quantum Network", Physical Review Letters **120**, 030501 (2018).

[45]J. Yin et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres", Nature **582**, 501 (2020).

[46]L. Chen et al., "Report on Post-Quantum Cryptography", NIST Interagency/Internal Report (NISTIR), 8105 (2016).

[47]B. Yurke, S. L. McCall, and J. R. Klauder, "SU(2) and SU(1,1) interferometers", Physical Review A **33**, 4033 (1986).

[48]C. M. Caves, "Quantum-mechanical noise in an interferometer", Physical Review D **23**, 1693 (1981).

[49]R. Schnabel, "Squeezed states of light and their applications in laser interferometers", Physics Reports **684**, 1 (2017).

[50]LIGO Caltech, *Facts | LIGO Lab | Caltech*, https://www.ligo.caltech.edu/page/facts.

[51]ESA/NASA, *LISA - Laser Interferometer Space Antenna*, https://lisa.nasa.gov/.

[52]J. P. Dowling and K. P. Seshadreesan, "Quantum Optical Technologies for Metrology, Sensing, and Imaging", Journal of Lightwave Technology **33**, 2359 (2015).

[53]R. A. Fisher, "Theory of Statistical Estimation", Mathematical Proceedings of the Cambridge Philosophical Society **22**, 700 (1925).

[54]C. W. Helstrom, "Quantum detection and estimation theory", Journal of Statistical Physics **1**, 231 (1969).

[55]A. Datta, R. Demkowicz-Dobrzański, and J. Liu, “Quantum multiparameter estimation and metrology—preface”, Journal of Physics A: Mathematical and Theoretical **54**, 460301 (2021).

[56]F. Albarelli, J. F. Friel, and A. Datta, “Evaluating the Holevo Cramér-Rao Bound for Multiparameter Quantum Metrology”, Physical Review Letters **123**, 200503 (2019).

[57]T. P. Heavner et al., “First accuracy evaluation of NIST-F2”, Metrologia **51**, 174 (2014).

[58]N. W. Spellmeyer et al., “Precision synchronization for free-space quantum networking”, in Quantum Computing, Communication, and Simulation III, edited by P. R. Hemmer and A. L. Migdall (Mar. 2023), p. 40.

[59]K. Boone et al., “Entanglement over global distances via quantum repeaters with satellite links”, Physical Review A **91**, 052325 (2015).

[60]J.-M. Mol et al., “Quantum memories for fundamental science in space”, Quantum Science and Technology **8**, 024006 (2023).

[61]NIST, *Transducers | Physical Measurement Laboratory*, https://www.nist.gov/pml/quantum-networks-nist/technologies-quantum-networks/transducers.

[62]C. Zhong, X. Han, and L. Jiang, “Microwave and Optical Entanglement for Quantum Transduction with Electro-Optomechanics”, Physical Review Applied **18**, 054061 (2022).

[63]A. Kumar et al., “Quantum-enabled millimetre wave to optical transduction using neutral atoms”, Nature **615**, 614 (2023).

[64]M. Caleffi and A. S. Cacciapuoti, “Quantum Switch for the Quantum Internet: Noiseless Communications Through Noisy Channels”, IEEE Journal on Selected Areas in Communications **38**, 575 (2020).

[65]C. Elliott, “The DARPA Quantum Network”, arXiv, quant–ph/0412029 (2004).

[66]J. Chung et al., “Illinois Express Quantum Network (IEQNET): metropolitan-scale experimental quantum networking over deployed optical fiber”, in Quantum information science, sensing, and computation xiii, edited by M. Hayduk and E. Donkor (Apr. 2021).

[67]R. Valivarthi et al., “Teleportation Systems Toward a Quantum Internet”, PRX Quantum **1**, 020317 (2020).

[68]AFRL, *Daytime Quantum Communication*, https://afresearchlab.com/technology/daytime-quantum-communication/.

[69]M. T. Gruneisen et al., “Modeling daytime sky access for a satellite quantum key distribution downlink”, Optics Express **23**, 23924 (2015).

[70]R. N. Lanning et al., “Quantum Communication over Atmospheric Channels: A Framework for Optimizing Wavelength and Filtering”, Physical Review Applied **16**, 044027 (2021).

[71]M. T. Gruneisen et al., “Adaptive spatial filtering of daytime sky noise in a satellite quantum key distribution downlink receiver”, Optical Engineering **55**, 026104 (2016).

[72]M. T. Gruneisen, B. A. Sickmiller, and M. B. Flanagan, “Modeling satellite-Earth quantum channel downlinks with adaptive-optics coupling to single-mode fibers”, in Quantum Information Science and Technology III, edited by M. T. Gruneisen, M. Dusek, and J. G. Rarity (Oct. 2017), p. 13.

[73]T. Jennewein et al., “QEYSSat 2.0 – White Paper on Satellite-based Quantum Communication Missions in Canada”, arXiv, 2306.02481 (2023).

[74]A. Villar et al., “Entanglement demonstration on board a nano-satellite”, Optica **7**, 734 (2020).

[75]L. Knips et al., “QUBE – Towards quantum key distribution with small satellites”, in Quantum 2.0 conference and exhibition (2022), QTh3A.6.

[76]ESA, *Space photons bring a new dimension to cryptography*, (May 2018) https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Space_photons_bring_a_new_dimension_to_cryptography.

[77]Z. Zhang and Q. Zhuang, “Distributed quantum sensing”, Quantum Science and Technology **6**, 043001 (2021).

[78]K. Akiyama et al. (The Event Horizon Telescope Collaboration), “First M87 Event Horizon Telescope Results. I. The Shadow of the Supermassive Black Hole”, The Astrophysical Journal Letters **875**, L1 (2019).

[79]D. Gottesman, T. Jennewein, and S. Croke, “Longer-Baseline Telescopes Using Quantum Repeaters”, Physical Review Letters **109**, 070503 (2012).

[80]E. T. Khabiboulline et al., “Optical Interferometry with Quantum Networks”, Physical Review Letters **123**, 070504 (2019).

[81]P. Kómár et al., “A quantum network of clocks”, Nature Physics **10**, 582 (2014).

[82]Y. Xia et al., “Quantum-Enhanced Data Classification with a Variational Entangled Sensor Network”, Physical Review X **11**, 021047 (2021).

[83]S. Weinberg, “A New Light Boson?”, Physical Review Letters **40**, 223 (1978).

[84]A. J. Brady et al., “Entangled Sensor-Networks for Dark-Matter Searches”, PRX Quantum **3**, 030333 (2022).

[85]M. Caleffi et al., “Distributed quantum computing: a survey”, arXiv, 2212.10609 (2022).

[86]S. Brandhofer, I. Polian, and K. Krsulich, “Optimal partitioning of quantum circuits using gate cuts and wire cuts”, IEEE Transactions on Quantum Engineering, 1 (2023).

[87]J. Clark, H. Thapliyal, and T. S. Humble, “A novel approach to quantum circuit partitioning”, in 2022 ieee computer society annual symposium on vlsi (isvlsi) (2022), pp. 450–451.

[88]A. Nakayama et al., “VQE-generated Quantum Circuit Dataset for Machine Learning”, arXiv, 2302.09751 (2023).

[89]J. F. Fitzsimons, “Private quantum computation: an introduction to blind quantum computing and related protocols”, npj Quantum Information **3**, 1 (2017).

[90]A. M. Childs, “Secure assisted quantum computation”, Quantum Info. Comput. **5**, 456 (2005).

[91]U. Mahadev, “Classical verification of quantum computations”, SIAM Journal on Computing **51**, 1172 (2022).

[92]A. Gheorghiu, T. Metger, and A. Poremba, *Quantum cryptography with classical communication: parallel remote state preparation for copy-protection, verification, and more*, Cryptology ePrint Archive, Paper 2022/122, https://eprint.iacr.org/2022/122, 2022.

[93]A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation", in 2009 50th annual ieee symposium on foundations of computer science (2009), pp. 517–526.

[94]J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation", Physical Review A **96**, 012303 (2017).

[95]C. Greganti et al., "Demonstration of measurement-only blind quantum computing", New Journal of Physics **18**, 013020 (2016).

[96]M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Device-Independent Verifiable Blind Quantum Computation", arXiv, 1502.02563 (2015).

[97]A. Gheorghiu, P. Wallden, and E. Kashefi, "Rigidity of quantum steering and one-sided device-independent verifiable quantum computation", New Journal of Physics **19**, 023043 (2017).

[98]A. Gheorghiu, E. Kashefi, and P. Wallden, "Robustness and device independence of verifiable blind quantum computing", New Journal of Physics **17**, 083040 (2015).

[99]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 **439**, 553 (1997).

[100]L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack", Physical Review Letters **79**, 325 (1997).

[101]S. Barz et al., "Demonstration of Blind Quantum Computing", Science **335**, 303 (2012).

[102]S. Barz et al., "Experimental verification of quantum computation", Nature Physics **9**, 727 (2013).

[103]L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Limitations on information-theoretically-secure quantum homomorphic encryption", Physical Review A **90**, 050303 (2014).

[104]S. Wiesner, "Conjugate coding", ACM SIGACT News **15**, 78 (1983).

[105]D. Gottesman and I. Chuang, "Quantum Digital Signatures", arXiv, quant–ph/0105032 (2001).

[106]J. Bartusek and D. Khurana, "Cryptography with certified deletion", in *Lecture notes in computer science* (Springer Nature Switzerland, 2023), pp. 192–223.

[107]A. Broadbent and R. Islam, "Quantum encryption with certified deletion", in *Lecture notes in computer science* (Springer International Publishing, 2020), pp. 92–122.

[108]G. Murta et al., "Quantum Conference Key Agreement: A Review", Advanced Quantum Technologies **3**, 2000025 (2020).

[109]M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing", Physical Review A **59**, 1829 (1999).

[110]M. Ben-Or and A. Hassidim, "Fast quantum byzantine agreement", in Proceedings of the thirty-seventh annual ACM symposium on Theory of computing (May 2005), pp. 481–485.

[111]C. H. Bennett et al., “Practical Quantum Oblivious Transfer”, in *Advances in Cryptology — CRYPTO ’91*, Vol. 576, edited by J. Feigenbaum (Springer Berlin Heidelberg, Berlin, Heidelberg, 1992), pp. 351–366.

[112]NASA, *NASA TechPort - Project Data*, https://techport.nasa.gov/view/94990.