Ofcom
making communications work
for everyone

Quantum Communications: new potential for the future of communications

Executive summary

Publication Date: 28 July 2021

Contents

Section

Annex

1. Overview

Purpose

1.1 Ofcom is the UK's independent communications regulator. We regulate the TV and radio sectors, fixed line telecoms, mobiles, postal services, plus the airwaves over which wireless devices operate.

1.2 Ofcom's Emerging Technology programme exists to conduct research and monitor industry and technological developments. This helps us to remain informed about new advances in technology and the impact that they might have on the sectors that we regulate.

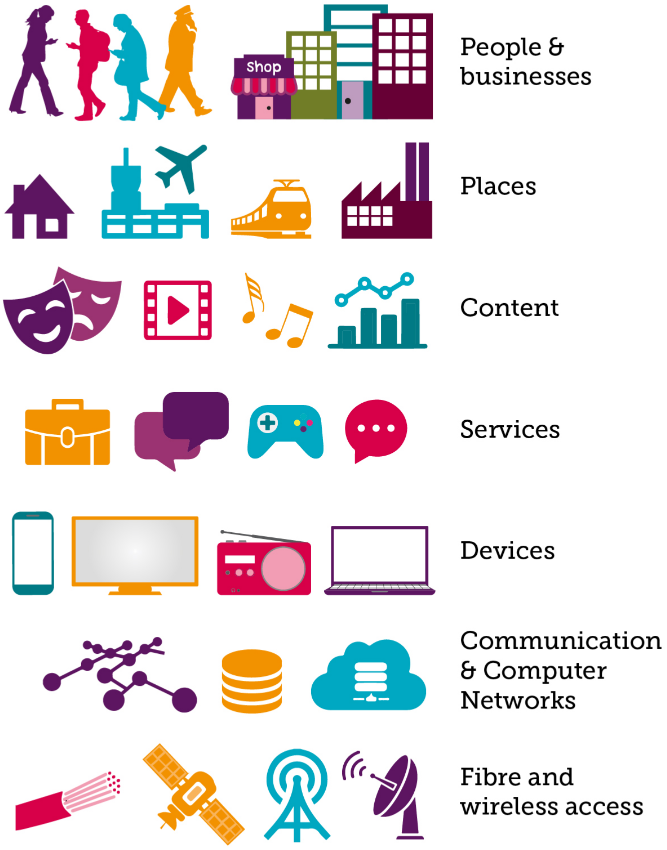

Figure 1: Scope of Ofcom's emerging technology programme. Source: Ofcom.

1.3 The objectives of the Emerging Technology programme include assessing the impact of technology and supporting technical developments across the sectors we regulate, by:

a) Providing strategic insights

b) Influencing standards when appropriate to support Ofcom's objectives

c) Providing technology advice to government and other policy makers

d) Reducing barriers to the introduction and adoption of new technologies consistent with policy goals

e) Tracking and assessing the impact of any changes to the technical architecture of networks

1.4 In our Emerging Technology Programme, Ofcom has identified various priority areas to help and support the growth of new technologies. The application of quantum physics principles to networks and communication could potentially impact on several of the sectors we regulate. Our Technology Futures report [Tech Futures, 2021], identified that technologies founded on the principles of quantum physics might have significant applications in security, computing, and communication.

1.5 Ofcom is also monitoring the progress of projects such as the UK National Quantum Technologies [UK National Quantum Technologies] programme which supports innovation in quantum research to move into industry-led applications that can benefit consumers and businesses.

1.6 Earlier this year, UK Research and Innovation (UKRI) expanded its programme [UK Research and Innovation] to set aside grants worth £153 million, supported by £205 million from industry, to develop new products and technologies based on advances made in quantum.

1.7 Government has launched an AI and quantum computing centre with IBM [AI & quantum computing, 2021]. This will include a government investment of £172 million over 5 years through UKRI, with an additional £38 million being invested by IBM.

1.8 Such initiatives that collaborate investment and expertise between multiple players have resulted in very interesting outcomes for quantum communication. For example, we have seen promising developments in addressing engineering challenges - Toshiba [Toshiba, 2021] with Cambridge Research Laboratory managed to extend the distance at which their quantum cryptography solution works in a fibre optic cable to 600km.

1.9 Based on these developments, we commissioned a report to provide greater understanding of the potential impact of advances in quantum physics on communication networks and set out how potentially these advances would translate to use cases across the sectors we regulate.

Background

1.10 Quantum mechanics refers to the branch of physics which deals with the behaviour of matter and light on the atomic and subatomic scale. It attempts to describe and account for the properties of molecules, atoms and their constituent particles, as well as photons, the subatomic particles of light. At this level, particles behave in strange ways, taking on more than one quantum state at the same time and interacting with other particles that may be very far away. This is largely due to the properties of *quantum superposition and entanglement.*

1.11 Quantum communication would use:

a) the property of **superposition** exhibited by quantum particles, which allows them to take on the properties of waves with no well-defined position or state. This effect can be exploited to perform certain calculations more efficiently. Unlike classical bits, quantum bits or qubits, can exist in multiple states, allowing them to perform multiple calculations at once, while classical bits are confined to a single state, a 0 or a 1. Moreover, quantum particles can travel along multiple communication lines simultaneously. This provides greater flexibility in the approach taken to communication that can make the information less susceptible to errors during transmission.

b) the principle of **entanglement**, which means, when a set of particles are generated or interact, in such a way that the quantum state of each particle of the group cannot be described independently of the state of the others, even when the particles are separated by a large distance. Researchers exploit entanglement to transfer quantum information across large distances; in this set-up the sender holds half of the entangled photons and the receiver holds the other half. Quantum information is transferred by using a combination of entanglement and classical communication.

1.12 By leveraging these fundamentals of quantum mechanics, quantum-based emerging technologies and use cases have the potential to grow at an accelerated pace. Ofcom is specifically interested in understanding which of the key communication sectors are using quantum technologies, so that we can track the pace of growth and understand what benefits this may bring to people and businesses.

1.13 We identified the following areas where advances in quantum physics could be most relevant for the communication sectors.

a) **Quantum computing is necessary, on a simple level, for quantum communication.** Current computers manipulate individual bits, which store information as binary 0 and 1 states (referred to as classical states). Quantum computers leverage quantum mechanical phenomena to manipulate information by relying on quantum bits, or qubits. Taken together, quantum superposition and entanglement have the potential to enable new advances in computing power. For example, where a two-bit register in an ordinary computer can store only one of four binary configurations (00, 01, 10, or 11) at any given time, a quantum computer or quantum processor can access a wider set of states, which include superpositions (i.e. combinations of) each of the four classical states, as well as exotic states which include quantum entanglement. This increased state space proves useful for certain types of computation. In particular circumstances, computations with qubits can be performed up to a million times faster when compared to classical bits [Quantum computing, 2019]. In the future, this could even permit extremely fast ways of solving certain mathematical problems, such as factorisation of large numbers, putting current cryptographic protocols at risk. Quantum computers can also potentially improve techniques of interference and error correction that may not be resolved by conventional computing approaches [Quantum error correction, 2012]. It is crucial to note that in order to do any communication using quantum physics at all, some form of quantum processor (simple quantum computer) is required in order to generate and process the information being sent.

b) **Quantum key distribution (QKD) or Quantum cryptography** refers to sending encrypted data as classical bits over networks, while the keys to decrypt the information are *transmitted* (but not measured and retained) as quantum states, which guarantees that an eavesdropper can be detected [Quantum key distribution]. QKD provides a way of distributing and sharing cryptographic keys by encoding the information on single photons. In practice, each photon is encoded with information determined by states of the photon such as polarisation. Once transmitted, photons can be measured and read as a string of classical bits, yielding a secret key which is used for secure communication. Although nodes that send or receive information via photons remain vulnerable, QKD enables the possibility of secure communication against possible future advances in computational power. This is because it only relies on the laws of physics, rather than on assumptions about the computational capabilities of the eavesdropper. This is unlike current cryptographic protocols, which rely on computational power assumptions that are vulnerable to current 'intercept-now-decrypt-later' attacks and any future quantum computers capable of breaking the encryption. Application of QKD is already happening in a number of industries to safeguard and protect both sensitive client information and business critical data. Quantum secure conference calls are an example application, as demonstrated by researchers at Heriot-Watt University [Heriot-Watt University, 2021] where they shared keys simultaneously between the four parties separated by up to 50 km of optical fibre. However, secure key distribution is only one element in securing complex systems and wider aspects should be considered – see [National Cyber Security Centre, 2020]

c) **Quantum Secure Cryptography, also referred to as quantum-resistant or post-quantum cryptography (PQC) [Post-quantum cryptography, 2019],** describes cryptographic systems that are secure against both classical computers and currently known quantum algorithms, and can interoperate with existing communications protocols and networks. As we edge closer to a time when large-scale quantum computers will become a reality, traditional encryption methods are at risk. In theory, PQC would include algorithms that utilise mathematical concepts such as hash or lattice-based cryptography to be resilient to quantum computer-enabled attacks.

d) **Quantum communication** involves moving away from classical forms of communication to instead take advantage of the laws of quantum physics to communicate via the transmission of quantum states. Traditionally, data would be sent as classical bits representing 1s and 0s. Instead, quantum communication proposes photons of light for transmitting data along optical cables or free space, which can take on a state of superposition, which means they can represent combinations of 1 and 0 simultaneously. Quantum communication is essential for the possibility of performing distributed or cloud computing with quantum computers.

e) **Quantum assisted communication** refers to utilising the advances in quantum mechanics to optimise conventional communication systems to be faster, more efficient, reliable and secure. For example, using classical bits of information within qubits, that can exist in multiple states and transmitted for communication purposes. Quantum-assisted wireless communications can also take advantage of the extra computing power offered by quantum mechanics via quantum computers to find the most suitable resource allocation, resulting in the lowest possible level of co-channel interference across the network.

1.14 Although Ofcom is interested in all of the above areas, we wanted a report to focus on understanding the scope and applications of quantum communication and quantum assisted communication as explained in paragraph 1.13 d) & e).

1.15 Quantum physics could potentially enable systems to perform beyond the limits of classical Shannon theory by allowing information carriers to be in a superposition of different information states, e.g. 0 and 1 simultaneously. This is quantum communication, governed by *quantum Shannon theory.* A large body of research on quantum Shannon theory has been established since the 1970s. We are therefore also interested in identifying the major engineering challenges which will be involved in realising the potential of quantum Shannon theory.

1.16 In the last few years, researchers have proposed further advances where both information carriers and the communication channels can be in quantum superposition, i.e. a single information carrier can travel through multiple channels simultaneously [Chiribella and Kristjánsson, 2019; [Abbott and others, 2020]. We are therefore interested in understanding whether, in theory, the recent advances in quantum can take us even further beyond Shannon by establishing the fundamental limits and the potential of extending Shannon's theory to situations where different transmission lines can be combined in a quantum way [Chiribella and Kristjánsson, 2019]; [Abbott and others, 2020]. We are also interested in identifying the major engineering challenges which will be involved in realising that potential.

1.17 In particular, we want to understand better the recent advances that have implications both in (a) improving existing classical communications channels using quantum principles and (b) exploring new technologies where the information to be transmitted is itself required to be in a quantum state.

1.18 We searched and identified a number of different research pieces that were relevant to us in the field of quantum communication. Among the ones that delved into these questions, we found a paper on quantum Shannon theory [Chiribella and Kristjánsson, 2019]. Following an internal assessment, we approached the authors to explore the topic of quantum communications further.

1.19 This led us to the three-person team to work on the report attached as Annex A; Prof Giulio Chiribella and doctoral student Hlér Kristjánsson from the University of Oxford along with their experimental collaborator Robert Gardner, PhD student at Imperial College London.

a) Prof Giulio Chiribella is a world-leading expert on quantum information theory and foundations, with around 200 scientific publications and over 5000 citations. He is a full professor at the University of Hong Kong, and previously held the position of full professor at the University of Oxford, where he is now a visiting professor. His research interests include the generalisation of quantum communication to paradigms where the transmission lines themselves are combined in a quantum manner, thus exploring the ultimate limits of communication in a quantum setting. Prof Chiribella won the prestigious Hermann Weyl Prize in 2010, and has held various fellowships, including being chosen as one of the 1000 Talents of China (2012) and being appointed a CIFAR-Azrieli Global Scholar (2016), a Croucher Senior Research Fellow (2018) and an RGC Senior Research Fellow (2020).

b) Hlér Kristjánsson is a 3rd-year doctoral student at the University of Oxford, under the supervision of Prof Giulio Chiribella and Prof Jonathan Barrett, and holds an MSci degree in physics from Imperial College London. His research focuses on studying the communication capabilities arising when transmission lines are combined in a quantum configuration and, together with Prof Giulio Chiribella, co-authored one of the first systematic studies of such generalised communication scenarios [Chiribella and Kristjánsson, 2019] as well as several follow-up works [Kristjánsson and others, 2021]. Hlér won the first prize student poster award at the 19th Asian Quantum Information Science Conference (AQIS'19) in Seoul, South Korea (2019) and the best student talk award at the Q-Turn International Conference (2020), and was selected as an invited speaker at the 18th International Conference on Quantum Physics and Logic (QPL) in 2021.

c) Robert Gardner is a 2nd-year doctoral student at Imperial College London, supervised by Dr Steve Kolthammer, as part of the Controlled Quantum Dynamics Centre for Doctoral Training. His work is focused on the experimental generation of quantum light, with applications in a range of areas including random number generation and quantum communication. He has previously worked on an optical set-up for quantum neural networks [Gardner and others, 2017] and is currently collaborating with Prof Chiribella's group on the experimental implementation using single photons of the extension of quantum Shannon theory.

1.20 The attached report in Annex A, presents the findings from their technical work on how quantum physics enables the possibility of developing a new generation of communication technologies. *The opinions and conclusions stated within the subsequent sections and the report are those of the individuals who conducted the work and may not reflect the view of Ofcom or imply any future policy work in related areas. Ofcom is not responsible for the content or accuracy of these reports*.

2. Key findings

Summary

2.1 The key areas of focus for Ofcom are quantum communication and quantum assisted communication outlined earlier in section in 1.13 (d) and (e) and the attached report is a high-level summary of how quantum physics can potentially introduce a new generation of quantum based communication technologies and applications.

2.2 The report draws outs three main contributions which include:

a) Influence of quantum physics on classical communication techniques (sections 2.5-2.8)

b) Transmission of quantum states or the transmission of quantum information between quantum devices (sections 2.9-2.19) and

c) Engineering challenges associated with implementing quantum principles for communication (sections 2.20-2.22)

2.3 The full report, which includes the glossary, is attached as an annex to this paper. It includes a more detailed analysis of the key conclusions that are documented below in this section. It also covers some of the fundamentals like superposition and entanglement that underpin these advancements and how these are different to classical communication networks that are in place today.

2.4 The report builds on steady progress made by classical communication systems that has its foundations in Shannon theory [Shannon, 1948]. The report explores the possibilities described by quantum Shannon theory, which suggests information to be encoded in the states of quantum particles, allowing them to simultaneously carry multiple information states [Wilde, 2013]. This feature can enable both enhancements in the communication of classical data (2.2 a), as well as the new possibility of communicating quantum information (2.2 b). Recent advances suggest that quantum Shannon theory can be extended to apply not only to the information-carrying states of particles, but also to the propagation of the particles in space and time. This ability of quantum particles to propagate simultaneously through multiple communication lines can boost the communication rate of both classical and quantum data through noisy channels [Chiribella and Kristjánsson, 2019].

An important point when considering the conclusions for quantum technologies throughout this report is that they cannot always be directly compared to existing classical technologies as a benchmark. This is partly due to the fact that quantum technologies have not yet reached the maturity of existing classical technologies, and also in many cases because quantum principles have the potential to enable new types of technology solutions, whose applications do not exist classically.

What does quantum mechanics do for classical communication systems?

2.5 As suggested in paragraphs 1.15 & 1.16, Ofcom is interested in specific implications of quantum physics for improving existing classical communication systems. A typical classical communication setting would involve a source (Alice) that sends information (bits) via a communication channel (a medium such as free space or fibre optic cable) to the receiver (Bob). For such a communication setting to make use of quantum physics, we would see Alice send information via bits encoded in single photons (particles of light) to Bob. This would first involve encoding the state of the qubit Alice wants to send in some physical parameter (called 'degree of freedom') of a single photon, for example its polarisation (which can be e.g. horizontal or vertical, or something in between – this is the same property of light that is responsible for the mechanism of polaroid glasses).

2.6 Once Alice has encoded her qubit in the photon, it is sent to Bob through an optical fibre, free space (i.e. air or vacuum, either on Earth or via a satellite), or some other medium, described by a quantum channel. Finally, Bob can perform measurements on the polarisation (or other degree of freedom) to decode the message.

2.7 There are several indications that the use of quantum resources can boost the capacity of sending classical bits through transmission lines.

2.8 The report explores several theoretical concepts:

2.8.1 Depending on the noise[1], one qubit of information can be used as a single classical bit, and any quantum channel can be used to transmit classical bits.

2.8.2 An interesting area is "superdense coding", which can potentially enable a sender and receiver to boost the capacity of the communication channel between them by up to a factor of 2, provided they share entangled quantum states prior to communication [Bennett and Wiesner, 1992]. In principle, this is a protocol which involves two entangled qubits, where Alice initially has one of the entangled qubits and Bob has the other. After appropriately encoding classical information in her qubit, Alice sends her qubit to Bob across a communication channel C. Bob can perform joint measurements on his initial qubit and the one which was sent to him by Alice, which yields two bits of classical information – doubling the number of bits that could have been transferred using the communication channel C alone, without the entangled state. Importantly, the information received by Bob can be controlled by Alice via her choice of encoding at the start of the protocol.

2.8.3 In theory, the rate of sending classical information can be improved through entanglement of successive qubits and this property of the transmission rate of quantum channels is known as "superadditivity" [superadditivity, 2009]. However, only very specific quantum channels are superadditive, and so far, all the channels corresponding to real-life communication systems are not superadditive, i.e.

[1] where noise is the refers to any unwanted change in the quantum state during transmission resulting in an error.

researchers are yet to entangle successive qubits to improve the communication rate.

2.8.4 The use of classical states of light together with non-classical (i.e. quantum) measurement techniques has been theoretically shown to achieve a higher capacity through various realistic quantum channel models with Gaussian noise compared to using only classical measurement techniques [Giovannetti and others, 2004]. Quantum physics enables successive qubits to be measured simultaneously in a quantum way, allowing new methods of light detection. For example, for a line-of-sight free-space optical channel, using these quantum measurement techniques yields up to a factor of 4 higher capacity than using traditional classical techniques [Shapiro, 2009].

2.8.5 The use of multiple transmission lines simultaneously, i.e. in a quantum superposition, has been shown to be able to increase the classical capacity of certain quantum channels. For example, when two discrete qubit white noise channels, each with zero capacity individually, are used in a quantum superposition, their combined capacity can be up to 0.31 bits per channel use [Abbott and others., 2020].

However, at present these results are primarily theoretical with some experimental proofs of principle, and only in the long term will it become clear to what extent, and in what scenarios, their benefit will outweigh the costs of using the quantum resources such as entangled states, non-classical measurement techniques, etc.

Transmission of quantum states or the transmission of quantum information between quantum devices

2.9 In addition to classical bits, quantum communication channels can also directly transfer quantum states (qubits) between a sender and receiver. In a future where multiple quantum computers at different locations need to share information to work together, the reliable communication of qubits between them will be important. Three key example use-cases are distributed quantum computing, quantum cloud computing, and ultraprecise GPS. These all require the construction of large-scale quantum communication networks between distant locations.

2.10 While in the previous section we considered the case of the transmission of classical bits encoded in qubits, here we consider the case where Alice and Bob exchange qubits and these qubits are not used to encode classical bits, i.e. they can be directly processed via quantum computers. This set-up is typical of a quantum network, where different quantum computers communicate between each other using a quantum channel. A key difference between the transmission of classical bits and qubits is that entanglement can be transmitted only with a qubit. This means that if the initial qubit Alice sent was entangled with another qubit in her lab, then the entanglement can be maintained when Bob receives it. This allows Alice and Bob to carry out quantum computational tasks which require entanglement between distant parties, for example distributed quantum computing.

2.11 In the short-to-medium term, many practical implementations of quantum communications networks are focused on QKD (out of scope of this report), described above in (1.13 b). However, in the long term, building communication networks for quantum communication would mean constructing an intercontinental quantum network i.e. the "quantum internet" – connecting quantum processors around the world. The quantum internet would realise in a global setting the key use-cases of distributed quantum computing, quantum cloud computing, and ultraprecise GPS.

2.12 Key use-cases of the communication of quantum information:

a) Distributed quantum computing (DQC). The advent of quantum computing opens the potential to solve hard or resource-intensive computational problems, with applications ranging from cybersecurity to financial modelling and drug discovery. However, as in the case of conventional computers, many computational problems require the combined effort of multiple interconnected processors, for example in distributed systems. DQC refers to connecting multiple small-scale quantum processors to form an effective larger, more powerful quantum computer. This will enable it to take advantage of superior resources and processing power by implementing quantum algorithms on distributed hardware to solve computational problems which may be intractable on individual quantum processors. [Quantum Internet, 2018]

b) Quantum cloud computing. Quantum computers in the future are expected to perform a similar function to today's supercomputers, in the sense that typically only large institutions will have one on-site, whilst access to them is provided remotely via the cloud. Quantum cloud computing refers to forming a quantum cloud from a network of locally hosted processors, which can be accessed by distant users in a similar way to classical cloud computing. [Quantum cloud computing, 2018]

c) Ultraprecise and ultra secure quantum clocks/GPS refers to using precision meteorology with quantum networks to operate a network of distant atomic clocks across large geographic distances, at close to the fundamental physical limit of precision. This uses entangled quantum states and quantum communication between the clocks to enable the possibility of extremely precise clock synchronization and GPS, which also potentially improves security against both internal and external threats. [Quantum clocks, 2014]

2.13 There is research [Bennett and others, 1996], that suggests that transmission of quantum information through a noisy quantum channel can be enhanced by allowing access to a classical channel in addition to the noisy quantum channel used to send the quantum information. This is an advantage as existing classical communication channels can enable an easier transmission of information compared to quantum channels that are still very early in their development cycle.

2.14 The report also draws attention to the concept of quantum teleportation whereby a quantum state can be transmitted, without using a physical medium to physically transmit the state. However, this requires (a) an entangled state to be shared between the sender and receiver (so the entangled state will have to be physically transmitted at an earlier time) and (b) classical communication between the sender and receiver.

2.15 A quantum network consists of a set of end nodes at various locations, connected via quantum communication channels, for example optical fibres. To allow for long-distance communication, the communication channels are connected via quantum repeaters. See Figure 2 below that illustrates a basic quantum network.

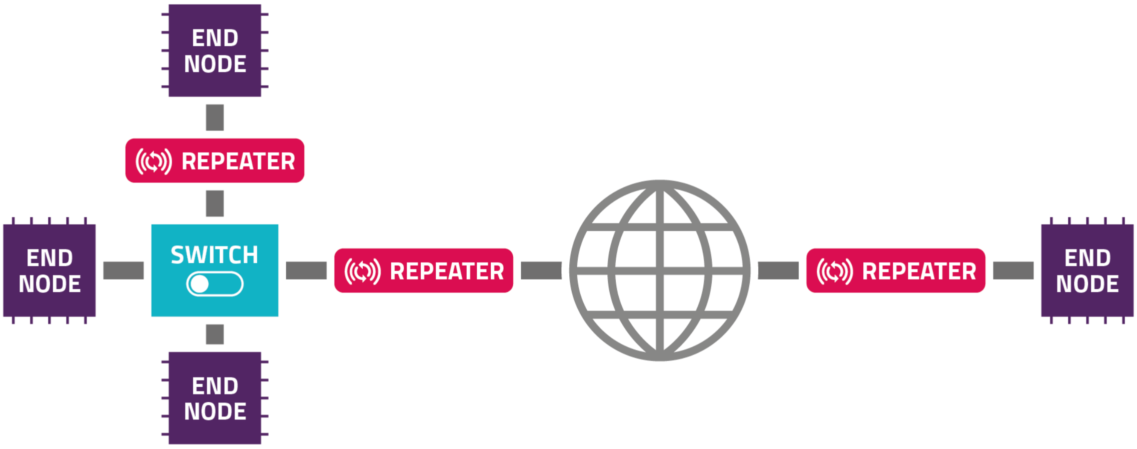

Figure 2: A schematic diagram of a worldwide quantum communication network. The end nodes (quantum computers) are connected via quantum channels grey lines and repeaters. A switch controls which end nodes to transmit to.

2.16 Unlike in classical communication systems, where signals are detected, amplified, and retransmitted, in the case of quantum, this is not possible as it is prevented by

a) the no-cloning theorem (an unknown quantum state cannot be copied) and

b) the fact that measurements collapse the quantum state into one of the classical outcomes.

2.17 The report highlights the importance of quantum repeaters that can potentially overcome this problem by discarding the need for a photon to be sent across the entire distance between the sender and receiver. Instead, the quantum repeater allows for the possibility of distributing an entangled state across adjacent nodes which would allow them to communicate quantum information using quantum teleportation [Gisin, 2015].

2.18 To establish such a communication channel, it would require transmitting quantum particles directly between the nodes (most commonly photons) through optical fibres or free space. To enable quantum communication, the nodes and repeaters should be able to operate directly on the photons. The end nodes of the network need to be designed to perform quantum information processing on the transmitted data in order to encode and decode the transmitted information. At the simplest level this would just involve generation and detection (measurements) of individual qubits but can range to fully fledged quantum computation for more complex applications. Information processing will generally be implemented via whatever medium is most convenient.

2.19 Existing quantum computing techniques typically encode information in static quantum particles, e.g. atoms, and not flying qubits (quantum particles that move through optical fibres or free space, such as photons) and a more efficient working of a quantum network would require the use of components such as quantum transducers. These are devices that enable the transfer of quantum information between different systems i.e. act as an interface between the static and flying qubits [Caleffi and others, 2018]. Such interface technologies are also required for quantum repeaters and memories – equally important components in a quantum network.

Engineering challenges when exploring the potential for quantum in communication

2.20 The majority of the engineering challenges discussed in this section are relevant to both pure quantum and quantum assisted classical forms of communication. This is because quantum networks typically work on the principle of sending single photons of light through optical fibres or free space. Information is encoded in controllable parameters of the photons, for example in their polarisation. Furthermore, it is possible to encode qubits into novel states of light instead of using single photons, for example coherent states (which correspond to classical light generated by a laser) and squeezed states (which are a quantum form of light).

2.21 In order to probe the nature of light at quantum level, the sender and receiver require access to specialised generation and detection devices, respectively, allowing them to control the properties of individual photons. Detection and generation of quantum light is an ongoing area of research, often requiring specific engineering practices such as cryogenic temperatures (on the order of 0-3 kelvin) for generators and detectors or quantum processors to encode and decode messages onto/from the states of successive photons.

2.22 This has been explored in the report and is summarised below.

2.22.1 **Appropriate Encoding Schemes:** We can choose to encode quantum information into photons in various ways, by taking advantage of the various degrees of freedom available to photons; and the report outlines these options in detail each with their own inherent advantages and disadvantages, e.g. polarisation, time-bins, frequency, etc. How we determine which encoding scheme could be used is based on two key areas:

a. *Suitability for quantum communication*: Impact on data bandwidth, capacity, security, and ease of transfer. The focus here is on the transfer of quantum information, as opposed to classical information.

b. *Suitability for performing useful quantum protocols*: Important factors include but are not limited to ease of photon interference, entanglement, or scalability.[2]

2.22.2 **Quantum state generation:** A set of parameters such as wavelength or photon length, needs to be controlled in order for photons to act effectively as carriers of quantum information. Additionally, for ease of quantum state generation, we also need to consider whether the process followed is deterministic or probabilistic and if cryogenic conditions are required. These parameters are detailed in the report and summarised below

2.22.3 Additionally, to perform algorithms of interest, photons will be required to interact with one another, which typically requires them to be indistinguishable and the report briefly outlines the variety of different physical methods for generating single photon states.

2.22.4 **Quantum state transmission:** The report also highlights the need to consider attenuation and loss of single photons over different mediums such as free space, fibres or satellite-ground links.

a. Unlike in the case of classical communications, where high energy radio frequency waves are often used to overcome loss limitations, this is not possible for transmission of single photons, whose energy is proportional to the photon’s frequency and therefore much lower for radio frequencies than for light. Ground-to-space communications is a viable option as loss levels are much lower. Engineering improvements to optical fibre loss, photon generation rates and detection efficiencies offer one route to improving transmission distances, although currently this yield diminishing returns because the loss is exponential. Techniques such as squeezed states that use multiphoton state to overcome the limitations of distance are a possibility in the longer term.

b. Another alternative is applying quantum theories of entanglement and the teleportation protocol directly, through the use of quantum memories and repeaters. For example, current state of the art memories allow storage of quantum information over the order of milliseconds, while it is expected that this will need to increase to the order of seconds to be useable in a quantum communication network [Bhaskar and others, 2020], [Wallucks and others, 2020].

[2] Scalability is just the ability to build bigger systems that can combine in order to perform more involved computations / protocols.

c. Satellite links have been used to demonstrate quantum information transmission over the range of 1000 km at reasonable transfer rates [Yin and others, 2018]. Distances of up to 7000 km have been demonstrated, although the transfer rate of single photons is limited to 1 photon every 200s [Dequal and others, 2016]. Using satellite links can mitigate losses due to atmospheric noise and absorption [Aspelmeyer and others, 2003] because photons mainly (beyond 10km above sea level) travel in an environment similar to a vacuum. In addition, the atmosphere is less likely to induce errors in polarisation-encoded qubits compared to fibre links.

2.22.5 **Quantum state detection:** For the purposes of photon detection, the report further examines a set of key parameters such as efficiency[3] and includes whether detectors are photon number resolving (i.e. can distinguish between different numbers of photons). The current generation of detectors are cryogenic so that is an additional constraint.

2.22.6 For communication systems, the focus is on single photon states, and the report reviews the existing approaches focusing particularly on their implementation and feasibility with useful examples. The majority of the current research involves techniques that focus on sending successive single photons; other techniques such as squeezed states that use multiphoton state have not been considered in detail as they are still in early phases of research.

[3] Efficiency: this is the probability that a photon, upon hitting the detector, triggers an electrical signal and thus yields a successful measurement. Ideally this should be 100%, but, in practice, this is reduced due to photon loss and imperfect photon coupling in the detector system.

3. References

Purpose

1. [Tech Futures, 2021] Technology Futures Report https://www.ofcom.org.uk/consultations-and-statements/category-2/emerging-technologies
2. [UK National Quantum Technologies] https://uknqt.ukri.org/
3. [UK Research and Innovation] Commercialising quantum technologies https://www.ukri.org/our-work/our-main-funds/industrial-strategy-challenge-fund/artificial-intelligence-and-data-economy/commercialising-quantum-technologies-challenge/
4. [AI & quantum computing, 2021]https://www.gov.uk/government/news/new-210-million-centre-to-create-jobs-of-the-future-with-ai-and-quantum-computing
5. [Toshiba, 2021] https://www.eurekalert.org/pub_releases/2021-06/tc-tab060421.php

Background

6. [Quantum Computing, 2019] https://www.nature.com/articles/s41586-019-1666-5.pdf
7. [Quantum error correction, 2012] https://www.sciencedirect.com/topics/engineering/quantum-error
8. [Quantum Key Distribution] https://uknqt.ukri.org/files/quantum-key-distribution/
9. [Heriot-Watt University, 2021] https://phys.org/news/2021-06-quantum-key-conference.html
10. [Post-quantum cryptography, 2019] https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography/
11. [National Cyber Security Centre, 2020] https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
12. [Chiribella and Kristjánsson, 2019] https://arxiv.org/pdf/1812.05292.pdf
13. [Kristjánsson and others, 2021] https://arxiv.org/pdf/1910.08197.pdf https://arxiv.org/pdf/2004.06090.pdf https://arxiv.org/pdf/2007.05005.pdf
14. [Gardner and others, 2017] https://arxiv.org/abs/1612.01045

Summary

15. [Shannon, 1948] https://ieeexplore.ieee.org/document/6773024 Shannon, C. E. (1948). A mathematical theory of communication. The Bell system technical journal, 27(3):379–423.
16. [Wilde, 2013]. https://arxiv.org/pdf/1106.1445.pdf

Quantum for classical communication

17. [Bennett and Wiesner, 1992] https://courses.physics.illinois.edu/phys513/sp2016/reading/week9/PhysRevLett.69.2881.pdf
18. [superadditivity, 2009] https://www.nature.com/articles/nphys1224.pdf
19. [Giovannetti and others, 2004] https://arxiv.org/pdf/quant-ph/0308012.pdf
20. [Shapiro, 2009] https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5223603&casa_token=A50NYrjAUwYAAAAA:CGsfCTsL6wagEQLg3-n0mlvZUHP9fzYRYAtb7npL2AcAvUltrxn4G2wMif5Je-7TS_M01iXK&tag=1
21. [Abbott and others, 2020] Abbott, A. A., Wechs, J., Horsman, D., Mhalla, M., & Branciard, C. (2020). Communication through coherent control of quantum channels. *Quantum*, *4*, 333. https://quantum-journal.org/papers/q-2020-09-24-333/pdf

Quantum communication

22. [Quantum Internet, 2018] S Wehner, D Elkouss, R Hanson, Quantum Internet: A vision for the road ahead, Science 2018 https://science.sciencemag.org/content/362/6412/eaam9288
23. [Quantum cloud computing, 2018] https://dl.acm.org/doi/pdf/10.1145/3233188.3233224?casa_token=qkS7yP3pMiwAAAAA:TINST9Ai3YvdGHEA7VWnyN8jpDbwvMmDp7-eRQOBbq0zko5ZqK5VIth7A7nYFkfPEtqHWDJglBcm
24. [Quantum clocks, 2014] A quantum network of clocks by P. Kómár et al. https://www.nature.com/articles/nphys3000.pdf
25. [Bennett and others, 1996] https://arxiv.org/pdf/quant-ph/9604024.pdf
26. [Gisin, 2015] https://link.springer.com/content/pdf/10.1007/s11467-015-0485-x.pdf
27. [Caleffi and others, 2018] https://dl.acm.org/doi/pdf/10.1145/3233188.3233224?casa_token=iT1qgMBLMjsAAAAA:ue9EgkDWm6-88_O_mQsjnPGLwlD60En8D3Yf5ueIpDWhGs_cJ2ZoGjl0ordVg_BX5HGPBDEV5ErB

Engineering challenges

28. [Bhaskar and others, 2020] https://arxiv.org/abs/1909.01323
29. [Wallucks and others, 2020] https://arxiv.org/abs/1910.07409
30. [Yin and others, 2019] https://arxiv.org/abs/1707.01339
31. [Dequal and others, 2016] https://arxiv.org/abs/1509.05692
32. [Aspelmeyer and others, 2003] https://arxiv.org/abs/quant-ph/0305105

A. Quantum Communications Report

Quantum communications report for Ofcom