

Workgroup: QIRG  
Internet-Draft:  
draft-irtf-qirg-quantum-internet-use-cases-08  
Published: 20 August 2021  
Intended Status: Informational  
Expires: 21 February 2022  
Authors: C. Wang  
InterDigital Communications, LLC  
A. Rahman  
InterDigital Communications, LLC  
R. Li M. Aelmans  
Kanazawa University Juniper Networks  
K. Chakraborty  
The University of Edinburgh  
**Application Scenarios for the Quantum Internet**

## **Abstract**

The Quantum Internet has the potential to improve application functionality by incorporating quantum information technology into the infrastructure of the overall Internet. This document provides an overview of some applications expected to be used on the Quantum Internet, and then categorizes them using various classification schemes. Some general requirements for the Quantum Internet are also discussed. The intent of this document is to describe a framework for applications, and describe a few selected application scenarios for the Quantum Internet. This document is a product of the Quantum Internet Research Group (QIRG).

## **Status of This Memo**

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 21 February 2022.

## Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

- [1. Introduction](#)
- [2. Terms and Acronyms List](#)
- [3. Quantum Internet Applications](#)
  - [3.1. Overview](#)
  - [3.2. Classification by Application Usage](#)
    - [3.2.1. Quantum Cryptography Applications](#)
    - [3.2.2. Quantum Sensing/Metrology Applications](#)
    - [3.2.3. Quantum Computing Applications](#)
  - [3.3. Control vs Data Plane Classification](#)
- [4. Selected Quantum Internet Application Scenarios](#)
  - [4.1. Secure Communication Setup](#)
  - [4.2. Secure Quantum Computing with Privacy Preservation](#)
  - [4.3. Distributed Quantum Computing](#)
- [5. General Requirements](#)
  - [5.1. Background](#)
  - [5.2. Requirements](#)
- [6. Conclusion](#)
- [7. IANA Considerations](#)
- [8. Security Considerations](#)
- [9. Acknowledgments](#)
- [10. Informative References](#)
- [Authors' Addresses](#)

## 1. Introduction

The Classical Internet has been constantly growing since it first became commercially popular in the early 1990's. It essentially consists of a large number of end-nodes (e.g., laptops, smart phones, network servers) connected by routers and clustered in Autonomous Systems. The end-nodes may run applications that provide service for the end-users such as processing and transmission of voice, video or data. The connections between the various nodes in

the Internet include backbone links (e.g., fiber optics) and access links (e.g., WiFi, cellular wireless, Digital Subscriber Lines (DSLs)). Bits are transmitted across the Classical Internet in packets.

Research and experiments have picked up over the last few years for developing the Quantum Internet [[Wehner](#)]. End-nodes will also be part of the Quantum Internet, in that case called quantum end-nodes that may be connected by quantum repeaters/routers. These quantum end-nodes will also run value-added applications which will be discussed later.

The connections between the various nodes in the Quantum Internet are expected to be primarily fiber optics and free-space optical lasers. Photonic connections are particularly useful because light (photons) is very suitable for physically realizing qubits. Qubits are expected to be transmitted across the Quantum Internet. The Quantum Internet will operate according to quantum physical principles such as quantum superposition and entanglement [[I-D.irtf-qirg-principles](#)].

The Quantum Internet is not anticipated to replace, but rather to enhance the Classical Internet. For instance, quantum key distribution can improve the security of the Classical Internet; the powerful computation capability of quantum computing can expedite and optimize computation-intensive tasks (e.g., routing modelling) in the Classical Internet. The Quantum Internet will run in conjunction with the Classical Internet to form a new Hybrid Internet. The process of integrating the Quantum Internet with the Classical Internet is similar to, but with more profound implications, as the process of introducing any new communication and networking paradigm into the existing Internet. The intent of this document is to provide a common understanding and framework of applications and application scenarios for the Quantum Internet.

This document represents the consensus of the Quantum Internet Research Group (QIRG). It has been reviewed extensively by Research Group (RG) members with expertise in both quantum physics and Classical Internet operation.

## **2. Terms and Acronyms List**

This document assumes that the reader is familiar with the quantum information technology related terms and concepts that are described in [[I-D.irtf-qirg-principles](#)]. In addition, the following terms and acronyms are defined herein for clarity:

\*Bell-Pairs - A special type of two-qubits quantum states. The two qubits show a correlation that cannot be observed in classical

information theory. We refer to such correlation as quantum entanglement. Bell-pairs exhibit the maximal quantum entanglement. One example of a Bell-pair is  $(|00\rangle + |11\rangle) / (\sqrt{2})$ . The Bell-pairs are a fundamental resource for quantum communication.

\*Bit - Binary Digit (i.e., fundamental unit of information in classical communications and classical computing).

\*Classical Internet - The existing, deployed Internet (circa 2020) where bits are transmitted in packets between nodes to convey information. The Classical Internet supports applications which may be enhanced by the Quantum Internet. For example, the end-to-end security of a Classical Internet application may be improved by secure communication setup using a quantum application.

\*Entanglement Swapping: It is a process of sharing an entanglement between two distant parties via some intermediate nodes. For example, suppose there are three parties A, B, C, and each of the parties (A, B) and (B, C) share Bell-pairs. B can use the qubits it shares with A and C to perform entanglement swapping operations, and as a result, A and C share Bell-pairs.

\*Fast Byzantine Negotiation - A Quantum-based method for fast agreement in Byzantine negotiations [[Ben-Or](#)] [[Taherkhani](#)].

\*Hybrid Internet - The "new" or evolved Internet to be formed due to a merger of the Classical Internet and the Quantum Internet.

\*Local Operations and Classical Communication (LOCC) - A method where nodes communicate in rounds, in which (1) they can send any classical information to each other; (2) they can perform local quantum operations individually; and (3) the actions performed in each round can depend on the results from previous rounds.

\*Noisy Intermediate-Scale Quantum (NISQ) - NISQ was defined in [[Preskill](#)] to represent a near-term era in quantum technology. According to this definition, NISQ computers have two salient features: (1) The size of NISQ computers range from 50 to a few hundred physical qubits (i.e., intermediate-scale); and (2) Qubits in NISQ computers have inherent errors and the control over them is imperfect (i.e., noisy).

\*Packet - Formatted unit of multiple related bits. The bits contained in a packet may be classical bits, or the measured state of qubits expressed in classical bits.

\*Prepare-and-Measure - A set of Quantum Internet scenarios where quantum nodes only support simple quantum functionalities (i.e.,

prepare qubits and measure qubits). For example, BB84 [BB84] is a prepare-and-measure quantum key distribution protocol.

- \*Quantum Computer (QC) - A quantum end-node that also has quantum memory and quantum computing capabilities is regarded as a full-fledged quantum computer.
- \*Quantum End-node - An end-node hosts user applications and interfaces with the rest of the Internet. Typically, an end-node may serve in a client, server, or peer-to-peer role as part of the application. If the end-node is part of a Quantum Network (i.e., is a quantum end-node), it must be able to generate/transmit and receive/process qubits. A quantum end-node must also be able to interface to the Classical Internet for control purposes and thus also be able to receive, process, and transmit classical bits/packets.
- \*Quantum Internet - A network of Quantum Networks. The Quantum Internet is expected to be merged into the Classical Internet to form a new Hybrid Internet. The Quantum Internet may either improve classical applications or may enable new quantum applications.
- \*Quantum Key Distribution (QKD) - A method that leverages quantum mechanics such as no-cloning theorem to let two parties (e.g., a sender and a receiver) securely establish/agree on a key.
- \*Quantum Network - A new type of network enabled by quantum information technology where qubits are transmitted between nodes to convey information. (Note: qubits must be sent individually and not in packets). The Quantum Network will use both quantum channels, and classical channels provided by the Classical Internet.
- \*Quantum Teleportation - A technique for transferring quantum information via local operations and classical communication (LOCC). If two parties share a Bell-pair, then using quantum teleportation a sender can transfer a quantum data bit to a receiver without sending it physically via a quantum communication channel.
- \*Qubit - Quantum Bit (i.e., fundamental unit of information in quantum communication and quantum computing). It is similar to a classic bit in that the state of a qubit is either "0" or "1" after it is measured, and is denoted as its basis state vector  $|0\rangle$  or  $|1\rangle$ . However, the qubit is different than a classic bit in that the qubit can be in a linear combination of both states before it is measured and termed to be in superposition. The

Degrees of Freedom (DOF) of a photon (e.g., polarization) or an electron (e.g., spin) can be used to encode a qubit.

### **3. Quantum Internet Applications**

#### **3.1. Overview**

The Quantum Internet is expected to be beneficial for a subset of existing and new applications. The expected applications for the Quantum Internet are still being developed as we are in the formative stages of the Quantum Internet [[Castelvecchi](#)] [[Wehner](#)]. However, an initial (and non-exhaustive) list of the applications to be supported on the Quantum Internet can be identified and classified using two different schemes. Note, this document does not include quantum computing applications that are purely local to a given node (e.g., quantum random number generator).

#### **3.2. Classification by Application Usage**

Applications may be grouped by the usage that they serve. Specifically, applications may be grouped according to the following categories:

- \*Quantum cryptography applications - Refers to the use of quantum information technology for cryptographic tasks such as quantum key distribution and quantum commitment.

- \*Quantum sensors applications - Refers to the use of quantum information technology for supporting distributed sensors (e.g., clock synchronization).

- \*Quantum computing applications - Refers to the use of quantum information technology for supporting remote quantum computing facilities (e.g., distributed quantum computing).

This scheme can be easily understood by both a technical and non-technical audience. The next sections describe the scheme in more detail.

##### **3.2.1. Quantum Cryptography Applications**

Examples of quantum cryptography applications include quantum-based secure communication setup and fast Byzantine negotiation.

1. Secure communication setup - Refers to secure cryptographic key distribution between two or more end-nodes. The most well-known method is referred to as Quantum Key Distribution (QKD) [[Renner](#)], which has been mathematically proven to be unbreakable.

2. Fast Byzantine negotiation - Refers to a Quantum-based method for fast agreement in Byzantine negotiations [[Ben-Or](#)], for example, to reduce the number of expected communication rounds and in turn achieve faster agreement, in contrast to classical Byzantine negotiations. A quantum aided Byzantine agreement on quantum repeater networks as proposed in [[Taherkhani](#)] includes optimization techniques to greatly reduce the quantum circuit depth and the number of qubits in each node. Quantum-based methods for fast agreement in Byzantine negotiations can be used for improving consensus protocols such as practical Byzantine Fault Tolerance(pBFT), as well as other distributed computing features which use Byzantine negotiations.
3. Quantum money - The main security requirement of money is unforgeability. A quantum money scheme aims to fulfill by exploiting the no-cloning property of the unknown quantum states. Though the original idea of quantum money dates back to 1970, these early protocols allow only the issuing bank to verify a quantum banknote. However, the recent protocols that are called public-key quantum money [[Zhandry](#)] allow anyone to verify the banknotes locally.

### **3.2.2. Quantum Sensing/Metrology Applications**

The entanglement, superposition, interference, squeezing properties can enhance the sensitivity of the quantum sensors and eventually can outperform the classical strategies. Examples of quantum sensor applications include network clock synchronization, high sensitivity sensing, quantum imaging, etc. These applications mainly leverage a network of entangled quantum sensors (i.e. quantum sensor networks) for high-precision multi-parameter estimation [[Proctor](#)].

1. Network clock synchronization - Refers to a world wide set of atomic clocks connected by the Quantum Internet to achieve an ultra precise clock signal [[Komar](#)] with fundamental precision limits set by quantum theory.
2. High sensitivity sensing - Refers to applications that leverage quantum phenomena to achieve reliable nanoscale sensing of physical magnitudes. For example, [[Guo](#)] uses an entangled quantum network for measuring the average phase shift among multiple distributed nodes.
3. Quantum imaging - The highly sensitive quantum sensors show great potential in improving the domain of magnetoencephalography. Unlike the current classical strategies, with the help of a network of quantum sensors, it is possible to measure the magnetic fields generated by the flow of current through neuronal assemblies in the brain while

the subject is moving. It reveals the dynamics of the networks of neurons inside the human brain on a millisecond timescale. This kind of imaging capability could improve the diagnosis and monitoring the conditions like attention-deficit-hyperactivity disorder [[Hill](#)].

### **3.2.3. Quantum Computing Applications**

In this section, we include the applications for the quantum computing. Note that, for the next couple of years we will have quantum computers as a cloud service. Sometimes, to run such applications in the cloud while preserving the privacy, the client and the server need to exchange qubits. Therefore, such privacy preserving quantum computing applications require a quantum internet to execute.

Examples of quantum computing include distributed quantum computing and secure quantum computing with privacy preservation, which can enable new types of cloud computing.

1. Distributed quantum computing - Refers to a collection of remote small capacity quantum computers (i.e., each supporting a relatively small number of qubits) that are connected and working together in a coordinated fashion so as to simulate a virtual large capacity quantum computer [[Wehner](#)].
2. Secure quantum computing with privacy preservation - Refers to private, or blind, quantum computation, which provides a way for a client to delegate a computation task to one or more remote quantum computers without disclosing the source data to be computed over [[Fitzsimons](#)].
3. Quantum chemistry - Quantum chemistry is one of the most promising quantum computing applications that can outperform the classical strategy using only a few hundred qubits quantum computers. Using the NISQ devices, the quantum algorithms manage to determine the molecular energies of the small molecules within chemical accuracy [[YudongCao](#)]. However, due to the short coherence time of the quantum devices, it is still difficult to simulate larger molecules.

### **3.3. Control vs Data Plane Classification**

The majority of routers currently used in the Classical Internet separate control plane functionality and data plane functionality for, amongst other reasons, stability, capacity and security. In order to classify applications for the Quantum Internet, a somewhat similar distinction can be made. Specifically some applications can be classified as being responsible for initiating sessions and performing other control plane functionality (including management



functionalities too). Other applications carry application or user data and can be classified as data plane functionality.

Some examples of what may be called control plane applications in the Classical Internet are Domain Name Server (DNS), Session Information Protocol (SIP), and Internet Control Message Protocol (ICMP). Furthermore, examples of data plane applications are E-mail, web browsing, and video streaming. Note that some applications may require both control plane and data plane functionality. For example, a Voice over IP (VoIP) application may use SIP to set up the call and then transmit the VoIP user packets over the data plane to the other party.

Similarly, nodes in the Quantum Internet applications may also use the classification paradigm of control plane functionality versus data plane functionality where:

\*Control Plane - Network functions and processes that operate on (1) control bits/packets or qubits (e.g., to setup up end-user encryption); or (2) management bits/packets or qubits (e.g., to configure nodes). For example, a quantum ping could be implemented as a control plane application to test and verify if there is a quantum connection between two quantum nodes. Another example is quantum superdense coding (which is used to transmit two classical bits by sending only one qubit). This approach does not need classical channels. Quantum superdense coding can be leveraged to implement a secret sharing application to share secrets between two parties [[ChuanWang](#)]. This secret sharing application based on quantum superdense encoding can be classified as control plane functionality.

\*Data Plane - Network functions and processes that operate on end-user application bits/packets or qubits (e.g., voice, video, data). Sometimes also referred to as the user plane. For example, a data plane application can be video conferencing, which uses QKD-based secure communication setup (which is a control plane function) to share a classical secret key for encrypting and decrypting video frames.

As shown in the table in [Figure 1](#), control and data plane applications vary for different types of networks. For a standalone Quantum Network (i.e., that is not integrated into the Internet), entangled qubits are its "data" and thus entanglement distribution can be regarded as its data plane application, while the signalling for controlling entanglement distribution be considered as control plane. However, looking at the Quantum Internet, QKD-based secure communication setup, which may be based on and leverage entanglement distribution, is in fact a control plane application, while video conference using QKD-based secure communication setup is a data

plane application. In the future, two data planes may exist, respectively for Quantum Internet and Classical Internet, while one control plane can be leveraged for both Quantum Internet and Classical Internet.

	Classical Internet Examples	Quantum Internet Examples	Hybrid Internet Examples
Control Plane	ICMP; DNS	Quantum ping; Signalling for controlling entanglement distribution;	QKD-based secure communication setup
Data Plane	Video conference	QKD; Entanglement distribution	Video conference using QKD-based secure communication setup

Figure 1: Examples of Control vs Data Plane Classification

#### 4. Selected Quantum Internet Application Scenarios

The Quantum Internet will support a variety of applications and deployment configurations. This section details a few key application scenarios which illustrates the benefits of the Quantum Internet. In system engineering, a application scenario is typically made up of a set of possible sequences of interactions between nodes and users in a particular environment and related to a particular goal. This will be the definition that we use in this section.

##### 4.1. Secure Communication Setup

In this scenario, two banks (i.e., Bank #1 and Bank #2) need to have secure communications for transmitting important financial transaction records (see [Figure 2](#)). For this purpose, they first need to securely share a classic secret cryptographic key (i.e., a sequence of classical bits), which is triggered by an end-user banker at Bank #1. This results in a source quantum node A at Bank #1 to securely establish a classical secret key with a destination quantum node B at Bank #2. This is referred to as a secure communication setup. Note that the quantum node A and B may be either a bare-bone quantum end-node or a full-fledged quantum

computer. This application scenario shows that the Quantum Internet can be leveraged to improve the security of Classical Internet applications of which the financial application shown in [Figure 2](#) is an example.

One requirement for this secure communication setup process is that it should not be vulnerable to any classical or quantum computing attack. This can be realized using QKD which has been mathematically proven to be information-theoretically secure and unbreakable. QKD can securely establish a secret key between two quantum nodes, using a classical authentication channel and insecure quantum communication channel without physically transmitting the key through the network and thus achieving the required security. However, care must be taken to ensure that the QKD system is safe against physical side channel attacks which can compromise the system. An example of a physical side channel attack is when an attacker is able to surreptitiously inject additional light into the optical devices used in QKD to learn side information about the system such as the polarization. Other specialized physical attacks against QKD have also used a classical authentication channel and insecure quantum communication channel such as the phase-remapping attack, photon number splitting attack, and decoy state attack [[Zhao](#)].

QKD is the most mature feature of the quantum information technology, and has been commercially released in small-scale and short-distance deployments. More QKD use cases are described in ETSI documents [[ETSI-QKD-UseCases](#)]; in addition, the ETSI document [[ETSI-QKD-Interfaces](#)] specifies interfaces between QKD users and QKD devices.

In general, the prepare and measure QKD protocols (e.g., [[BB84](#)]) without using entanglement works as follows:

1. The source quantum node A encodes classical bits to qubits. Basically, the source node A generates two random classical bit strings  $X$ ,  $Y$ . Among them, it uses the bit string  $X$  to choose the basis and uses  $Y$  to choose the state corresponding to the chosen basis. For example, if  $X=0$  then in case of BB84 protocol Alice prepares the state in  $\{|0\rangle, |1\rangle\}$ -basis; otherwise she prepares the state in  $\{|+\rangle, |-\rangle\}$ -basis. Similarly, if  $Y=0$  then Alice prepares the qubit either  $|0\rangle$  or  $|+\rangle$  (depending on the value of  $X$ ), and if  $Y=1$ , then Alice prepares the qubit either  $|1\rangle$  or  $|-\rangle$ .
2. The source quantum node A sends qubits to the destination quantum node B via quantum channel.

3. The destination quantum node receives qubits and measures each of them in one of the two basis at random.
4. The destination quantum node informs the source node of its choice of basis for each qubit.
5. The source quantum node informs the destination node which random quantum basis is correct.
6. Both nodes discard any measurement bit under different quantum basis and remaining bits could be used as the secret key. Before generating the final secret key, there is a post-processing procedure over authenticated classical channels. The classical post-processing part can be subdivided into three steps, namely parameter estimation, error-correction, and privacy amplification. In the parameter estimation phase, both Alice and Bob use some of the bits to estimate the channel error. If it is larger than some threshold value, then they abort the protocol otherwise move to the error-correction phase. Basically, if an eavesdropper tries to intercept and read qubits sent from node A to node B, the eavesdropper will be detected due to the entropic uncertainty relation property theorem of quantum mechanics. As a part of the post-processing procedure, both nodes usually also perform information reconciliation [[Elkouss](#)] for efficient error correction and/or conduct privacy amplification [[BTang](#)] for generating the final information-theoretical secure keys.
7. The post-processing procedure needs to be performed over an authenticated classical channel. In other words, the source quantum node and the destination quantum node need to authenticate the classical channel to make sure there is no eavesdroppers or man-in-the-middle attacks, according to certain authentication protocols such as [[Kiktenko](#)]. In [[Kiktenko](#)], the authenticity of the classical channel is checked at the very end of the post-processing procedure instead of doing it for each classical message exchanged between the quantum source node and the quantum destination node.

It is worth noting that:

1. There are some entanglement-based QKD protocols such as [[Treiber](#)], which work differently than above steps. The entanglement-based schemes, where entangled states are prepared externally to the source quantum node and the destination quantum node, are not normally considered "prepare-and-measure" as defined in [[Wehner](#)]; other entanglement-based schemes, where entanglement is generated within the source quantum node can

still be considered "prepare-and-measure"; send-and-return schemes can still be "prepare-and-measure", if the information content, from which keys will be derived, is prepared within the source quantum node the source quantum node before being sent to the destination quantum node for measurement.

2. There are many enhanced QKD protocols based on [BB84]. For example, a series of loopholes have been identified due to the imperfections of measurement devices; there are several solutions to take into account these attacks such as measurement-device-independent QKD [PZhang]. These enhanced QKD protocols can work differently than the steps of BB84 protocol [BB84].
3. For large-scale QKD, QKD Networks (QKDN) are required, which can be regarded as a subset of a Quantum Internet. A QKDN may consist of a QKD application layer, a QKD network layer, and a QKD link layer [Qin]. One or multiple trusted QKD relays [QZhang] may exist between the source quantum node A and the destination quantum node B, which are connected by a QKDN. Alternatively, a QKDN may rely on entanglement distribution and entanglement-based QKD protocols; as a result, quantum-repeaters/routers instead of trusted QKD relays are needed for large-scale QKD.
4. Although the addresses of Source Quantum Node A and Destination Quantum Node B could be identified and exposed, the identity of users, who will use the secret cryptographic key for secure communications, will not necessarily be exposed during QKD process. In other words, there is no direct mapping from the addresses of quantum nodes to the user identity; as a result, QKD protocols do not disclose user identities.
5. QKD provides an information-theoretical way to share secret keys between two parties in the presence of Eve. However, this is true in theory, and there is a significant gap between theory and practice. By exploiting the imperfection of the detectors Eve can gain information about the shared key [FeihuXu]. To avoid such side-channel attacks in [Lo], the researchers provide a QKD protocol called Measurement Device-Independent (MDI) QKD that allows two users (a transmitter "Alice" and a receiver "Bob") to communicate with perfect security, even if the (measurement) hardware they are using has been tampered with (e.g., by an eavesdropper) and thus is not trusted. It is achieved by measuring correlations between signals from Alice and Bob rather than the actual signals themselves.

6. QKD protocols based on Continuous Variable (CV-QKD) have recently seen plenty of interest as it only requires telecommunications equipment that is readily available and is also in common use industry-wide. This kind of technology is a potentially high-performance technique for secure key distribution over limited distances. The recent demonstration of CV-QKD shows compatibility with classical coherent detection schemes that are widely used for high bandwidth classical communication systems [[Grosshans](#)] Note that we still do not have a quantum repeater for the continuous variable systems; hence, this kind of QKD technologies can be used for the short distance communications or trusted relay-based QKD networks.

As a result, the Quantum Internet in [Figure 2](#) contains quantum channels. And in order to support secure communication setup especially in large-scale deployment, it also requires entanglement generation and entanglement distribution [[I-D.van-meter-qirg-quantum-connection-setup](#)], quantum repeaters/routers, and/or trusted QKD relays.

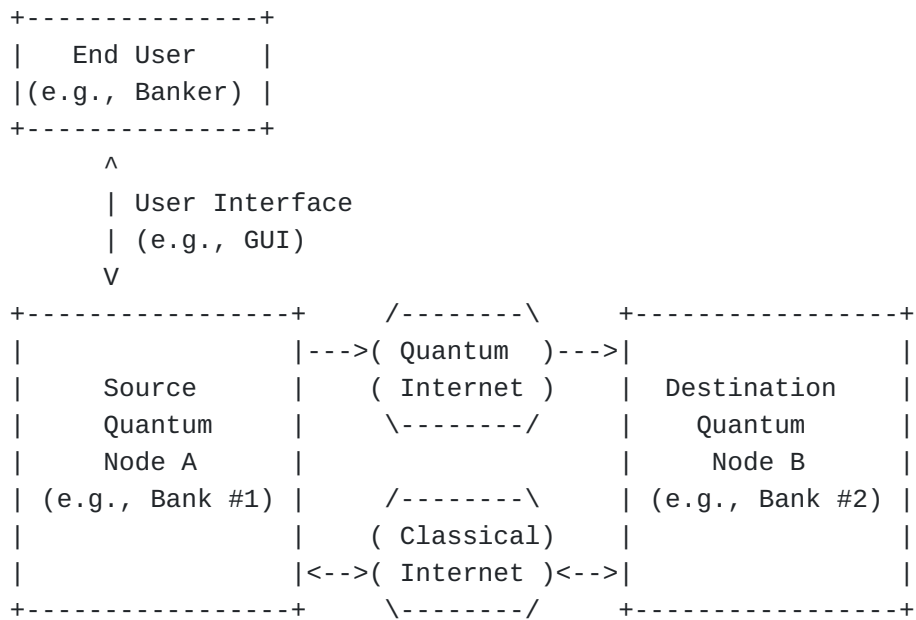


Figure 2: Secure Communication Setup

## 4.2. Secure Quantum Computing with Privacy Preservation

Secure computation with privacy preservation refers to the following scenario:

1. A client node with source data delegates the computation of the source data to a remote computation node (i.e. a server).
2. Furthermore, the client node does not want to disclose any source data to the remote computation node and thus preserve the source data privacy.
3. Note that there is no assumption or guarantee that the remote computation node is a trusted entity from the source data privacy perspective.

As an example illustrated in [Figure 3](#), a terminal node such as a home gateway has collected lots of data and needs to perform computation on the data. The terminal node could be a classical node without any quantum capability, a bare-bone quantum end-node or a full-fledged quantum computer. The terminal node has insufficient computing power and needs to offload data computation to some remote nodes. Although the terminal node can upload the data to the cloud to leverage cloud computing without introducing local computing overhead, to upload the data to the cloud can cause privacy concerns. In this particular case, there is no privacy concern since the source data will not be sent to the remote computation node which could be compromised. Many protocols as described in [\[Fitzsimons\]](#) for delegated quantum computing or Blind Quantum Computation (BQC) can be leveraged to realize secure delegated computation and guarantee privacy preservation simultaneously.

As a new client/server computation model, BQC generally enables: 1) The client delegates a computation function to the server; 2) The client does not send original qubits to the server, but send transformed qubits to the server; 3) The computation function is performed at the server on the transformed qubits to generate temporary result qubits, which could be quantum-circuit-based computation or measurement-based quantum computation. The server sends the temporary result qubits to the client; 4) The client receives the temporary result qubits and transform them to the final result qubits. During this process, the server can not figure out the original qubits from the transformed qubits. Also, it will not take too much efforts on the client side to transform the original qubits to the transformed qubits, or transform the temporary result qubits to the final result qubits. One of the very first BQC protocols such as [\[Childs\]](#) follows this process, although the client needs some basic quantum features such as quantum memory, qubit preparation and measurement, and qubit transmission. Measurement-

based quantum computation is out of the scope of this document and more details about it can be found in [[Jozsa](#)].

It is worth noting that:

1. The BQC protocol in [[Childs](#)] is a circuit-based BQC model, where the client only performs simple quantum circuit for qubit transformation, while the server performs a sequence of quantum logic gates. Qubits are transmitted back and forth between the client and the server.
2. Universal BQC in [[Broadbent](#)] is a measurement-based BQC model, which is based on measurement-based quantum computing leveraging entangled states. The principle in UBQC is based on the fact the quantum teleportation plus a rotated Bell measurement realizes a quantum computation, which can be repeated multiple times to realize a sequence of quantum computation. In this approach, the client first prepares transformed qubits and send them to the server and the server needs first to prepare entangled states from all received qubits. Then, multiple interaction and measurement rounds happen between the client and the server. For each round, the client computes and sends new measurement instructions or measurement adaptations to the server; then, the server performs the measurement according to the received measurement instructions to generate measurement results (qubits or in classic bits); the client receives the measurement results and transform them to the final results.
3. A hybrid universal BQC is proposed in [[XZhang](#)], where the server performs both quantum circuits like [[Childs](#)] and quantum measurements like [[Broadbent](#)] to reduce the number of required entangled states in [[Broadbent](#)]. Also, the client is much simpler than the client in [[Childs](#)]. This hybrid BQC is a combination of circuit-based BQC model and measurement-based BQC model.
4. It will be ideal if the client in BQC is a purely classical client, which only needs to interact with the server using classical channel and communications. [[HHuang](#)] demonstrates such an approach, where a classical client leverages two entangled servers to perform BQC, with the assumption that both servers can not communicate with each other; otherwise, the blindness or privacy of the client can not be guaranteed. The scenario as demonstrated in [[HHuang](#)] is essentially an example of BQC with multiple servers.
5. How to verify that the server will perform what the client requests or expects is an important issue in many BQC



protocols, referred to as verifiable BQC. [Fitzsimons] discusses this issue and compares it in various BQC protocols.

In [Figure 3](#), the Quantum Internet contains quantum channels and quantum repeaters/routers for long-distance qubits transmission [[I-D.irtf-qirg-principles](#)].

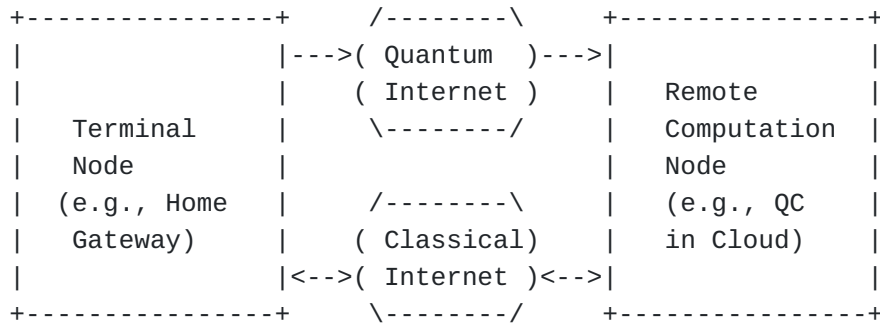


Figure 3: Secure Quantum Computing with Privacy Preservation

#### 4.3. Distributed Quantum Computing

There can be two types of distributed quantum computing [[Denchev](#)]:

1. Leverage quantum mechanics to enhance classical distributed computing problems. For example, entangled quantum states can be exploited to improve leader election in classical distributed computing, by simply measuring the entangled quantum states at each party (e.g., a node or a device) without introducing any classical communications among distributed parties [[Pal](#)]. Normally, pre-shared entanglement needs first be established among distributed parties, followed by LOCC operations at each party. And it generally does not need to transmit qubits among distributed parties.
2. Distribute quantum computing functions to distributed quantum computers. A quantum computing task or function (e.g., quantum gates) is split and distributed to multiple physically separate quantum computers. And it may or may not need to transmit qubits (either inputs or outputs) among those distributed quantum computers. Pre-shared entangled states may be needed to transmit quantum states among distributed quantum computers without using quantum communications, similar to quantum teleportation. For example, [[Gottesman](#)] and [[Eisert](#)] have proved that a CNOT gate can be realized jointly by and distributed to multiple quantum computers. The rest of this section focuses on this type of distributed quantum computing.

As a scenario for the second type of distributed quantum computing, Noisy Intermediate-Scale Quantum (NISQ) computers distributed in different locations are available for sharing. According to the definition in [Preskill], a NISQ computer can only realize a small number of qubits and has limited quantum error correction. In order to gain higher computation power before fully-fledged quantum computers become available, NISQ computers can be connected via classical and quantum channels. This scenario is referred to as distributed quantum computing [Caleffi] [Cacciapuoti01] [Cacciapuoti02]. This application scenario reflects the vastly increased computing power which quantum computers as a part of the Quantum Internet can bring, in contrast to classical computers in the Classical Internet, in the context of distributed quantum computing ecosystem [Cuomo]. According to [Cuomo], quantum teleportation enables a new communication paradigm, referred to as teledata [VanMeter01], which moves quantum states among qubits to distributed quantum computers. In addition, distributed quantum computation also needs the capability of remotely performing quantum computation on qubits on distributed quantum computers, which can be enabled by the technique called telegate [VanMeter02].

As an example, scientists can leverage these connected NISQ computer to solve highly complex scientific computation problems such as analysis of chemical interactions for medical drug development [Cao] (see Figure 4). In this case, qubits will be transmitted among connected quantum computers via quantum channels, while classic control messages will be transmitted among them via classical channels for coordination and control purpose. Another example of distributed quantum computing is secure Multi-Party Quantum Computation (MPQC) [Crepeau], which can be regarded as a quantum version of classical secure Multi-Party Computation (MPC). In a secure MPQC protocol, multiple participants jointly perform quantum computation on a set of input quantum states, which are prepared and provided by different participants. One of the primary aims of the secure MPQC is to guarantee that each participant will not know input quantum states provided by other participants. Secure MPQC relies on verifiable quantum secret sharing [Lipinska].

For the example shown in Figure 4, qubits from one NISQ computer to another NISQ computer are very sensitive and should not be lost. For this purpose, quantum teleportation can be leveraged to teleport sensitive data qubits from one quantum computer A to another quantum computer B. Note that Figure 4 does not cover measurement-based distributed quantum computing, where quantum teleportation may not be required. When quantum teleportation is employed, the following steps happen between A and B. In fact, LOCC [Chitambar] operations

are conducted at the quantum computer A and B in order to achieve quantum teleportation as illustrated in [Figure 4](#).

1. The quantum computer A locally generates some sensitive data qubits to be teleported to the quantum computer B.
2. A shared entanglement is established between the quantum computer A and the quantum computer B (i.e., there are two entangled qubits: q1 at A and q2 at B). For example, the quantum computer A can generate two entangled qubits (i.e., q1 and q2) and sends q2 to the quantum computer B via quantum communications.
3. Then, the quantum computer A performs a Bell measurement of the entangled qubit q1 and the sensitive data qubit.
4. The result from this Bell measurement will be encoded in two classical bits, which will be physically transmitted via a classical channel to the quantum computer B.
5. Based on the received two classical bits, the quantum computer B modifies the state of the entangled qubit q2 in the way to generate a new qubit identical to the sensitive data qubit at the quantum computer A.

In [Figure 4](#), the Quantum Internet contains quantum channels and quantum repeaters/routers [[I-D.irtf-qirg-principles](#)]. This application scenario needs to support entanglement generation and entanglement distribution (or quantum connection) setup [[I-D.van-meter-qirg-quantum-connection-setup](#)] in order to support quantum teleportation.

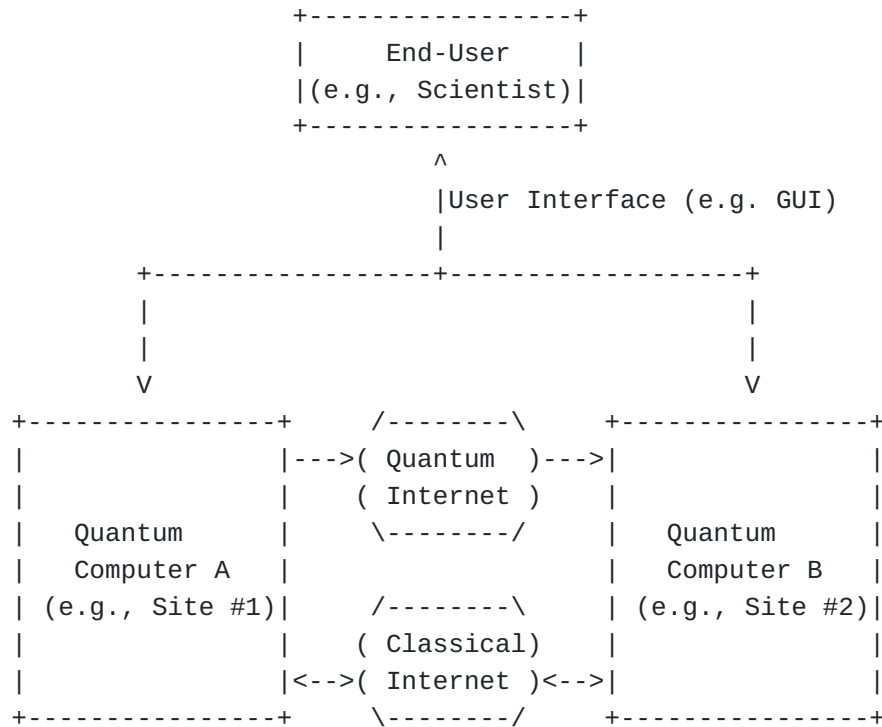


Figure 4: Distributed Quantum Computing

## 5. General Requirements

### 5.1. Background

Quantum technologies are steadily evolving and improving. Therefore, it is hard to predict the timeline and future milestones of quantum technologies as pointed out in [Grumblin] for quantum computing. Currently, a NISQ computer can achieve fifty to hundreds of qubits with some given error rate. In fact, the error rates of two-qubit quantum gates have decreased nearly in half every 1.5 years (for trapped ion gates) to 2 years (for superconducting gates). The error rate also increases as the number of qubits increases. For example, a current 20-physical-qubit machine has a total error rate which is close to the total error rate of a 7 year old two-qubit machine [Grumblin].

On the network level, six stages of Quantum Internet development are described in [Wehner] as follows:

1. Trusted repeater networks (Stage-1)
2. Prepare and measure networks (Stage-2)
3. Entanglement distribution networks (Stage-3)

4. Quantum memory networks (Stage-4)
5. Fault-tolerant few qubit networks (Stage-5)
6. Quantum computing networks (Stage-6)

The first stage is simple trusted repeater networks, while the final stage is the quantum computing networks where the full-blown Quantum Internet will be achieved. Each intermediate stage brings with it new functionality, new applications, and new characteristics. [Figure 5](#) illustrates Quantum Internet application scenarios as described in this document mapped to the Quantum Internet stages described in [\[Wehner\]](#). For example, secure communication setup can be supported in Stage-1, Stage-2, or Stage-3, but with different QKD solutions. More specifically:

In Stage-1, basic QKD is possible and can be leveraged to support secure communication setup but trusted nodes are required to provide end-to-end security. The primary requirement is the trusted nodes.

In Stage-2, the end users can prepare receive and measure the qubits. In this stage the users can verify classical passwords without revealing it.

In Stage-3, end-to-end security can be enabled based on quantum repeaters and entanglement distribution, to support the same secure communication setup application. The primary requirement is entanglement distribution to enable long-distance QKD.

In Stage-4, the quantum repeaters gain the capability of storing and manipulating entangled qubits in the quantum memories. Using these kind of quantum networks one can run sophisticated applications like blind quantum computing, leader election, quantum secret sharing.

In Stage-5, quantum repeaters can perform error correction; hence they can perform fault-tolerant quantum computations on the received data. With the help of these repeaters, it is possible to run distributed quantum computing and quantum sensor applications over a smaller number of qubits.

Finally, in Stage-6, distributed quantum computing relying on more qubits can be supported.

Quantum Internet Stage	Example Quantum Internet Use Cases	Characteristic
Stage-1	Secure comm setup using basic QKD	Trusted nodes
Stage-2	Secure comm setup using the QKD with end-to-end security	Prepare-and-measure capability
Stage-3	Secure comm setup using entanglement-enabled QKD	Entanglement distribution
Stage-4	Secure/blind quantum computing	Quantum memory
Stage-5	Higher-Accuracy Clock synchronization	Fault tolerance
Stage-6	Distributed quantum computing	More qubits

Figure 5: Example Application Scenarios in Different Quantum Internet Stages

## 5.2. Requirements

Some general and functional requirements on the Quantum Internet from the networking perspective, based on the above application scenarios, are identified as follows:

1. Methods for facilitating quantum applications to interact efficiently with entangled qubits are necessary in order for them to trigger distribution of designated entangled qubits to potentially any other quantum node residing in the Quantum Internet. To accomplish this, specific operations must be performed on entangled qubits (e.g., entanglement swapping, entanglement distillation). Quantum nodes may be quantum end-nodes, quantum repeaters/routers, and/or quantum computers.
2. Quantum repeaters/routers should support robust and efficient entanglement distribution in order to extend and establish high-fidelity entanglement connection between two quantum

nodes. For achieving this, it is required to first generate an entangled pair on each hop of the path between these two nodes, and then perform entanglement swapping operations at each of the intermediate nodes.

3. Quantum end-nodes must send additional information on classical channels to aid in transmission of qubits across quantum repeaters/receivers. This is because qubits are transmitted individually and do not have any associated packet overhead which can help in transmission of the qubit. Any extra information to aid in routing, identification, etc., of the qubit(s) must be sent via classical channels.
4. Methods for managing and controlling the Quantum Internet including quantum nodes and their quantum resources are necessary. The resources of a quantum node may include quantum memory, quantum channels, qubits, established quantum connections, etc. Such management methods can be used to monitor network status of the Quantum Internet, diagnose and identify potential issues (e.g. quantum connections), and configure quantum nodes with new actions and/or policies (e.g. to perform a new entanglement swapping operation). New management information model for the Quantum Internet may need to be developed.

## **6. Conclusion**

This document provides an overview of some expected application categories for the Quantum Internet, and then details selected application scenarios. The applications are first grouped by their usage which is a natural and easy to understand classification scheme. The applications are also classified as either control plane or data plane functionality as typical for the Classical Internet. This set of applications may, of course, naturally expand over time as the Quantum Internet matures. Finally, some general requirements for the Quantum Internet are also provided.

This document can also serve as an introductory text to readers interested in learning about the practical uses of the Quantum Internet. Finally, it is hoped that this document will help guide further research and development of the Quantum Internet functionality required to implement the application scenarios described herein.

## **7. IANA Considerations**

This document requests no IANA actions.

## 8. Security Considerations

This document does not define an architecture nor a specific protocol for the Quantum Internet. It focuses instead on detailing application scenarios, requirements, and describing typical Quantum Internet applications. However, some salient observations can be made regarding security of the Quantum Internet as follows.

It has been identified in [[NISTIR8240](#)] that once large-scale quantum computing becomes reality that it will be able to break many of the public-key (i.e., asymmetric) cryptosystems currently in use. This is because of the increase in computing ability with quantum computers for certain classes of problems (e.g., prime factorization, optimizations). This would negatively affect many of the security mechanisms currently in use on the Classical Internet which are based on public-key (Diffie-Hellman) encryption. This has given strong impetus for starting development of new cryptographic systems that are secure against quantum computing attacks [[NISTIR8240](#)].

Interestingly, development of the Quantum Internet will also mitigate the threats posed by quantum computing attacks against Diffie-Hellman based public-key cryptosystems. Specifically, the secure communication setup feature of the Quantum Internet as described in [Section 4.1](#) will be strongly resistant to both classical and quantum computing attacks against Diffie-Hellman based public-key cryptosystems.

A key additional threat consideration for the Quantum Internet is pointed to by [[RFC7258](#)], which warns of the dangers of pervasive monitoring as a widespread attack on privacy. Pervasive monitoring is defined as a widespread, and usually covert, surveillance through intrusive gathering of application content or protocol metadata such as headers. This can be accomplished through active or passive wiretaps, traffic analysis, or subverting the cryptographic keys used to secure communications.

The secure communication setup feature of the Quantum Internet as described in [Section 4.1](#) will be strongly resistant to pervasive monitoring based on directly attacking (Diffie-Hellman) encryption keys. Also, [Section 4.2](#) describes a method to perform remote quantum computing while preserving the privacy of the source data. Finally, the intrinsic property of qubits to decohere if they are observed, albeit covertly, will theoretically allow detection of unwanted monitoring in some future solutions.



## 9. Acknowledgments

The authors want to thank Michele Amoretti, Mathias Van Den Bossche, Xavier de Foy, Patrick Gelard, Alvaro Gomez Inesta, Wojciech Kozlowski, John Mattsson, Rodney Van Meter, Joey Salazar, and Joseph Touch, and the rest of the QIRG community as a whole for their very useful reviews and comments to the document.

## 10. Informative References

- [BB84] Bennett, C. H. and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", 1984, <<http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf>>.
- [Ben-Or] Ben-Or, M. and A. Hassidim, "Fast Quantum Byzantine Agreement", SOTC, ACM, 2005, <<https://dl.acm.org/doi/10.1145/1060590.1060662>>.
- [Broadbent] Broadbent, A. and et. al., "Universal Blind Quantum Computation", 50th Annual Symposium on Foundations of Computer Science, IEEE, 2009, <<https://arxiv.org/pdf/0807.4154.pdf>>.
- [BTang] Tang, B. and et. al., "High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution", Scientific Reports, Nature Research, 2019, <<https://doi.org/10.1038/s41598-019-50290-1>>.
- [Cacciapuoti01] Cacciapuoti, A.S. and et. al., "Quantum Internet: Networking Challenges in Distributed Quantum Computing", IEEE Network, January 2020, 2020, <<https://ieeexplore.ieee.org/document/8910635>>.
- [Cacciapuoti02] Cacciapuoti, A.S. and et. al., "When Entanglement meets Classical Communications: Quantum Teleportation for the Quantum Internet", 2019, <<https://arxiv.org/abs/1907.06197>>.
- [Caleffi] Caleffi, M. and et. al., "Quantum internet: From Communication to Distributed Computing!", NANOCOM, ACM, 2018, <<https://dl.acm.org/doi/10.1145/3233188.3233224>>.
- [Cao] Cao, Y. and et. al., "Potential of Quantum Computing for Drug Discovery", Journal of Research and Development, IBM, 2018, <<https://doi.org/10.1147/JRD.2018.2888987>>.
- [Castelvecchi] Castelvecchi, D., "The Quantum Internet has arrived (and it hasn't)", Nature 554, 289-292, 2018, <<https://www.nature.com/articles/d41586-018-01835-3>>.

**[Childs]**

Childs, A. M., "Secure Assisted Quantum Computation", 2005, <<https://arxiv.org/pdf/quant-ph/0111046.pdf>>.

**[Chitambar]** Chitambar, E. and et. al., "Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask)", Communications in Mathematical Physics, Springer, 2014, <<https://link.springer.com/article/10.1007/s00220-014-1953-9>>.

**[ChuanWang]** Wang, C. and et. al., "Quantum Secure Direct Communication with High-Dimension Quantum Superdense Coding", Physical Review A, American Physical Society, 2005, <<https://doi.org/10.1103/PhysRevA.71.044305>>.

**[Crepeau]** Crepeau, C. and et. al., "Secure Multi-party Quantum Computation", 34th Symposium on Theory of Computing (STOC), ACM, 2002, <<https://doi.org/10.1145/509907.510000>>.

**[Cuomo]** Cuomo, D. and et. al., "Towards a Distributed Quantum Computing Ecosystem", Quantum Communication, IET, 2020, <<http://dx.doi.org/10.1049/iet-qtc.2020.0002>>.

**[Denchev]** Denchev, V.S. and et. al., "Distributed Quantum Computing: A New Frontier in Distributed Systems or Science Fiction?", SIGACT News ACM, 2018, <<https://doi.org/10.1145/1412700.1412718>>.

**[Eisert]** Eisert, J. and et. al., "Optimal Local Implementation of Nonlocal Quantum Gates", Physical Review A, American Physical Society, 2000, <<https://doi.org/10.1103/PhysRevA.101.032332>>.

**[Elkouss]** Elkouss, D. and et. al., "Information Reconciliation for Quantum Key Distribution", 2011, <<https://arxiv.org/pdf/1007.1616.pdf>>.

**[ETSI-QKD-Interfaces]** ETSI GR QKD 003 V2.1.1, "Quantum Key Distribution (QKD); Components and Internal Interfaces", 2018, <[https://www.etsi.org/deliver/etsi\\_gr/QKD/001\\_099/003/02.01.01\\_60/gr\\_QKD003v020101p.pdf](https://www.etsi.org/deliver/etsi_gr/QKD/001_099/003/02.01.01_60/gr_QKD003v020101p.pdf)>.

**[ETSI-QKD-UseCases]** ETSI GR QKD 002 V1.1.1, "Quantum Key Distribution (QKD); Use Cases", 2010, <[https://www.etsi.org/deliver/etsi\\_gs/qkd/001\\_099/002/01.01.01\\_60/gs\\_qkd002v010101p.pdf](https://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf)>.

**[FeihuXu]** Xu, F. and et. al., "Experimental Demonstration of Phase-Remapping Attack in a Practical Quantum Key Distribution

System", New Journal of Physics, 12 113026, 2010, <<https://iopscience.iop.org/article/10.1088/1367-2630/12/11/113026>>.

[Fitzsimons] Fitzsimons, J. F., "Private Quantum Computation: An Introduction to Blind Quantum Computing and Related Protocols", 2017, <<https://www.nature.com/articles/s41534-017-0025-3.pdf>>.

[Gottesman] Gottesman, D. and I. Chuang, "Demonstrating the Viability of Universal Quantum Computation using Teleportation and Single-Qubit Operations", Nature 402, 390-393, 1999, <<https://doi.org/10.1038/46503>>.

[Grosshans] Grosshans, F. and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States", Physical Review Letters, American Physical Society, 2002, <<https://doi.org/10.1103/PhysRevLett.88.057902>>.

[Grumbling] Grumbling, E. and M. Horowitz, "Quantum Computing: Progress and Prospects", National Academies of Sciences, Engineering, and Medicine, The National Academies Press, 2019, <<https://doi.org/10.17226/25196>>.

[Guo] Guo, X. and et. al., "Distributed Quantum Sensing in a Continuous-Variable Entangled Network", Nature Physics, Nature, 2020, <<https://www.nature.com/articles/s41567-019-0743-x>>.

[HHuang] Huang, H. and et. al., "Experimental Blind Quantum Computing for a Classical Client", 2017, <<https://arxiv.org/pdf/1707.00400.pdf>>.

[Hill] Hill, R.M. and et. al., "A Tool for Functional Brain Imaging with Lifespan Compliance", Nature Communications 10, 4785(2019), 2019, <<https://doi.org/10.1038/s41467-019-12486-x>>.

[I-D.dahlberg-ll-quantum] Dahlberg, A., Skrzypczyk, M., and S. Wehner, "The Link Layer service in a Quantum Internet", Work in Progress, Internet-Draft, draft-dahlberg-ll-quantum-03, 10 October 2019, <<https://www.ietf.org/archive/id/draft-dahlberg-ll-quantum-03.txt>>.

[I-D.irtf-qirg-principles]

Kozlowski, W., Wehner, S., Meter, R. V., Rijsman, B., Cacciapuoti, A. S., Caleffi, M., and S. Nagayama, "Architectural Principles for a Quantum Internet", Work in Progress, Internet-Draft, draft-irtf-qirg-

principles-07, 4 June 2021, <<https://www.ietf.org/archive/id/draft-irtf-qirg-principles-07.txt>>.

- [**I-D.van-meter-qirg-quantum-connection-setup**] Meter, R. V. and T. Matsuo, "Connection Setup in a Quantum Network", Work in Progress, Internet-Draft, draft-van-meter-qirg-quantum-connection-setup-01, 11 September 2019, <<https://www.ietf.org/archive/id/draft-van-meter-qirg-quantum-connection-setup-01.txt>>.
- [**Jozsa**] Jozsa, R. and et. al., "An Introduction to Measurement based Quantum Computation", 2005, <<https://arxiv.org/pdf/quant-ph/0508124.pdf>>.
- [**Kiktenko**] Kiktenko, E.O. and et. al., "Lightweight Authentication for Quantum Key Distribution", 2020, <<https://arxiv.org/pdf/1903.10237.pdf>>.
- [**Komar**] Komar, P. and et. al., "A Quantum Network of Clocks", 2013, <<https://arxiv.org/pdf/1310.6045.pdf>>.
- [**Lipinska**] Lipinska, V. and et. al., "Verifiable Hybrid Secret Sharing with Few Qubits", Physical Review A, American Physical Society, 2020, <<https://doi.org/10.1103/PhysRevA.101.032332>>.
- [**Lo**] Lo, H.-K. and et. al., "Experimental Demonstration of Phase-Remapping Attack in a Practical Quantum Key Distribution System", Physical Review Letters, American Physical Society, 2012, <<https://doi.org/10.1103/PhysRevLett.108.130503>>.
- [**NISTIR8240**] Alagic, G. and et. al., "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process", NISTIR 8240, 2019, <<https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf>>.
- [**Pal**] Pal, S.P. and et. al., "Multi-partite Quantum Entanglement versus Randomization: Fair and Unbiased Leader Election in Networks", 2003, <<https://arxiv.org/pdf/quant-ph/0306195.pdf>>.
- [**Preskill**] Preskill, J., "Quantum Computing in the NISQ Era and Beyond", 2018, <<https://arxiv.org/pdf/1801.00862>>.
- [**Proctor**] Proctor, T.J. and et. al., "Multiparameter Estimation in Networked Quantum Sensors", Physical Review Letters, American Physical Society, 2018, <<https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.080501>>.

**[PZhang]**

Zhang, P. and et. al., "Integrated Relay Server for Measurement-Device-Independent Quantum Key Distribution", 2019, <<https://arxiv.org/abs/1912.09642>>.

**[Qin]**

Qin, H., "Towards Large-Scale Quantum Key Distribution Network and Its Applications", 2019, <[https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Hao\\_Qin\\_Presentation.pdf](https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Hao_Qin_Presentation.pdf)>.

**[QZhang]**

Zhang, Q., Hu, F., Chen, Y., Peng, C., and J. Pan, "Large Scale Quantum Key Distribution: Challenges and Solutions", Optical Express, OSA, 2018, <<https://doi.org/10.1364/OE.26.024260>>.

**[Renner]**

Renner, R., "Security of Quantum Key Distribution", 2006, <<https://arxiv.org/pdf/quant-ph/0512258.pdf>>.

**[RFC2119]**

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

**[RFC7258]**

Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <<https://www.rfc-editor.org/info/rfc7258>>.

**[Taherkhani]**

Taherkhani, M.A., Navi, K., and R. Van Meter, "Resource-Aware System Architecture Model for Implementation of Quantum Aided Byzantine Agreement on Quantum Repeater Networks", Quantum Science and Technology, IOP, 2017, <<https://dl.acm.org/doi/10.1145/1060590.1060662>>.

**[Treiber]**

Treiber, A. and et. al., "A Fully Automated Entanglement-based Quantum Cryptography System for Telecom Fiber Networks", New Journal of Physics, 11, 045013, 2009, <<https://doi.org/10.1364/OE.26.024260>>.

**[VanMeter01]**

Van Meter, R. and et. al., "Distributed Arithmetic on a Quantum Multicomputer", 33rd International Symposium on Computer Architecture (ISCA) IEEE, 2006, <<https://doi.org/10.1109/ISCA.2006.19>>.

**[VanMeter02]**

Van Meter, R. and et. al., "Architecture of a Quantum Multicomputer Optimized for Shor's Factoring Algorithm", 2006, <<https://arxiv.org/pdf/quant-ph/0607065.pdf>>.

**[Wehner]**

Wehner, S., Elkouss, D., and R. Hanson, "Quantum internet: A vision for the road ahead", Science 362,

2018, <<http://science.sciencemag.org/content/362/6412/eaam9288.full>>.

**[XZhang]** Zhang, X. and et. al., "A Hybrid Universal Blind Quantum Computation", Information Sciences, Elsevier, 2009, <<https://www.sciencedirect.com/science/article/abs/pii/S002002551930458X>>.

**[YudongCao]** Cao, Y. and et. al., "Quantum Chemistry in the Age of Quantum Computing", Chemical Reviews, ACS Publications, 2019, <<https://doi.org/10.1021/acs.chemrev.8b00803>>.

**[Zhandry]** Zhandry, M., "Quantum Lightning Never Strikes the Same State Twice", 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III, 2019, <[http://doi.org/10.1007/978-3-030-17659-4\\_14](http://doi.org/10.1007/978-3-030-17659-4_14)>.

**[Zhao]** Zhao, Y., "Development of Quantum Key Distribution and Attacks against it", Journal of Physics, J. Phys, 2018, <<https://iopscience.iop.org/article/10.1088/1742-6596/1087/4/042028>>.

#### Authors' Addresses

Chonggang Wang  
InterDigital Communications, LLC  
1001 E Hector St  
Conshohocken, 19428  
United States of America

Email: [Chonggang.Wang@InterDigital.com](mailto:Chonggang.Wang@InterDigital.com)

Akbar Rahman  
InterDigital Communications, LLC  
1000 Sherbrooke Street West  
Montreal H3A 3G4  
Canada

Email: [rahmansakbar@yahoo.com](mailto:rahmansakbar@yahoo.com)

Ruidong Li  
Kanazawa University  
Kakuma-machi,  
Ishikawa Prefecture 920-1192  
Japan

Email: [lrd@se.kanazawa-u.ac.jp](mailto:lrd@se.kanazawa-u.ac.jp)

Melchior Aelmans

Juniper Networks  
Boeing Avenue 240  
Schiphol-Rijk

Email: [maelmans@juniper.net](mailto:maelmans@juniper.net)

Kaushik Chakraborty  
The University of Edinburgh  
10 Crichton Street  
Edinburgh  
EH8 9AB, Scotland  
United Kingdom

Email: [kchakrab@exseed.ed.ac.uk](mailto:kchakrab@exseed.ed.ac.uk)