QIRG
Internet-Draft
Intended status: Informational
Expires: November 6, 2020

C. Wang
A. Rahman
InterDigital Communications, LLC
R. Li
NICT
M. Aelmans
Juniper Networks

May 5, 2020

Applications and Use Cases for the Quantum Internet
draft-wang-qirg-quantum-internet-use-cases-06

Abstract

The Quantum Internet has the potential to improve Internet application functionality by incorporating quantum information technology into the infrastructure of the overall Internet. In this document, we provide an overview of some applications expected to be used on the Quantum Internet, and then categorize them using various classification schemes. Some general requirements for the Quantum Internet are also discussed. The intent of this document is to provide a common understanding and framework of applications and use cases for the Quantum Internet.

Status of This Memo

Copyright Notice

Table of Contents

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. 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 Digital Subscriber

Lines (DSLs), fiber optics, coax cable and wireless that include Bluetooth, WiFi, cellular (e.g., 3G, 4G, 5G), and satellite, etc. Bits are transmitted across the Classical Internet in packets.

Research and experimentation have picked up over the last few years for developing a Quantum Internet [Wehner]. It is anticipated that the Quantum Internet will provide intrinsic benefits such as better end-to-end and network security. The Quantum Internet will also have end-nodes, termed quantum end-nodes. Quantum end-nodes 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 optics. Photonic connections are particularly useful because light (photons) is very suitable for physically encoding qubits. Unlike the Classical Internet, qubits (and not classical bits or packets) are expected to be transmitted across the Quantum Internet due to the underlying physics. The Quantum Internet will operate according to unique physical principles such as quantum superposition, entanglement and teleportation [I-D.irtf-qirg-principles].

The Quantum Internet is not anticipated to replace the Classical Internet. For instance, Local Operations and Classical Communication (LOCC) operations [Chitambar] even rely on classical communications. Instead 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 use cases for the Quantum Internet.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. 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 here for clarity:

- Bit - Binary Digit (i.e., fundamental unit of information in a classical computer).

- 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.

- 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: 1) local quantum operations (e.g., quantum measurement) are performed at one quantum node A; 2) the quantum operation result is sent to another quantum node B via classical communications; 3) the quantum node B may also perform some local quantum operations dependent on the received operation result from the quantum node A. For example, LOCC can be used to transform entangled states into other entangled states.

- 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 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.

o 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 the Quantum Network, it must be able to generate/transmit and/or receive/process qubits. A quantum end-node, if it has quantum memory and quantum computing capabilities, can be regarded as a quantum computer. 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.

o Quantum Computer (QC) - Compared to a quantum end-node, a QC has more capabilities such as quantum memory and quantum circuits, which are required for performing quantum computing tasks.

o 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.

o Quantum Internet - A network of quantum networks. The Quantum Internet will 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.

o Qubit - Quantum Bit (i.e., fundamental unit of information in a quantum computer). 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 |0> or |1>. However, the qubit is different than a classic bit in that the qubit is 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.

4. Quantum Internet Applications

4.1. Overview

The Quantum Internet is expected to be extremely beneficial for a subset of existing and new applications. The expected applications using 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.

4.2. Classification by Application Usage

Applications may also be grouped by the usage that they serve into a tripartite classification. Specifically, applications may be classified according to the following usages:

- Quantum cryptography applications - Refers to the use of quantum information technology to ensure secure communications (e.g., QKD).

- Quantum sensors applications - Refers to the use of quantum information technology for supporting distributed sensors or Internet of Things (IoT) devices (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 is a useful classification scheme as it can be easily understood by both a technical and non-technical audience. Following are some more details.

4.2.1. 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].

2. Fast Byzantine negotiation - Refers to a quantum network based method for fast agreement in Byzantine negotiations [Fitzi].

This can be used for the popular financial blockchain feature as well as other distributed computing features which use Byzantine negotiations.

4.2.2. Quantum Sensor Applications

The main example of a quantum sensor applications is currently network clock synchronization.

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].

4.2.3. Quantum Computing Applications

Examples of quantum computing include distributed quantum computing and secure quantum computing with privacy preservation.

1. Distributed quantum computing - Refers to a collection of remote small capacity quantum computers (i.e., each supporting a few 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].

4.3. 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. 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 use the same classification paradigm of control plane functionality versus data plane functionality where:

- o 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).

- o 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.

5. Selected Quantum Internet Use Cases

The Quantum Internet will support a variety of applications and deployment configurations. This section details a few key use cases which illustrates the benefits of the Quantum Internet. In system engineering, a use case 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.

5.1. 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 1). For this purpose, they first need to securely exchange 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 send a classic secret key to 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 use case shows that the Quantum Internet can be leveraged to improve the security of Classical Internet applications of which the financial application shown in Figure 1 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 [ETSI-QKD-Interfaces]. QKD can securely establish a secret key between two quantum nodes, without physically transmitting it through the network and thus achieving the required security. QKD is the most mature feature of the quantum information technology, and has been commercially deployed in small-scale and short-distance deployments. More QKD use cases have been described in ETSI GS QKD 002 [ETSI-QKD-UseCases].

In general, QKD (e.g., [BB84]) without using entanglement works as follows:

1. The source quantum node A (e.g. Alice) transforms the secret key to qubits. Basically, for each classical bit in the secret key, the source quantum node A randomly selects one quantum computational basis and uses it to prepare/generate a qubit for the classical bit.

2. The source quantum node A sends qubits to the destination quantum node B (e.g. Bob) via quantum channel.

3. The destination quantum node receives qubits and measures them based on its random quantum basis.

4. The destination node informs the source node of its random quantum basis.

5. The source node informs the destination node which random quantum basis is correct.

6. Both nodes discard any measurement bit under different quantum basis and store all remaining bits as the secret key.

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 Alice and Bob, are not normally considered "prepare-and-measure" as defined in [Wehner]; other entanglement-based schemes, where entanglement is generated within Alice 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 Alice before being sent to Bob 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 [ZhangPeiyu]. These enhanced QKD protocol 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 [QinHao]. One or multiple trusted QKD relays [ZhangQiang] 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.

As a result, the Quantum Internet in Figure 1 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.

```
        +----------------+
        |    End User    |
        |(e.g., Banking  |
        |  Application)  |
        +----------------+
              ^
              | User Interface
              | (e.g., GUI)
              V
        +------------------+     /--------\     +------------------+
        |                  |--->( Quantum  )--->|                  |
        |      Source      |    ( Internet )    |   Destination    |
        |      Quantum     |     \--------/     |     Quantum      |
        |      Node A      |                    |      Node B      |
        | (e.g., Bank #1)  |     /--------\     | (e.g., Bank #2)  |
        |                  |    ( Classical)    |                  |
        |                  |<-->( Internet )<-->|                  |
        +------------------+     \--------/     +------------------+
```

Figure 1: Secure Communication Setup

5.2. Distributed Quantum Computing

In this scenario, 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 classic and quantum channels. This scenario is referred to as distributed quantum computing [Caleffi] [Cacciapuoti01] [Cacciapuoti02]. This use case 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.

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 (see Figure 2). 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. Qubits from one NISQ computer to another NISQ computer are very sensitive and cannot 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 2 does not cover measurement-based

distributed quantum computing, where quantum teleportation may not be required.

Specifically, 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 2.

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).

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 2, the Quantum Internet contains quantum channels and quantum repeaters/routers [I-D.irtf-qirg-principles]. This use case needs to support entanglement generation in order to enable quantum teleportation, entanglement distribution or quantum connection setup [I-D.van-meter-qirg-quantum-connection-setup] in order to support

long-distance quantum teleportation.


```
                          +-----------------+
                          |     End-User    |
                          |(e.g., Scientist)|
                          +-----------------+
                                    ^
                                    |User Interface (e.g. GUI)
                                    |
                +-------------------+-------------------+
                |                                       |
                |                                       |
                V                                       V
        +-----------------+      /--------\      +-----------------+
        |                 |--->( Quantum  )--->|                 |
        |                 |    ( Internet )    |                 |
        |   Quantum       |      \--------/      |   Quantum       |
        |   Computer A    |                      |   Computer B    |
        | (e.g., Site #1) |      /--------\      | (e.g., Site #2) |
        |                 |    ( Classical)    |                 |
        |                 |<-->( Internet )<-->|                 |
        +-----------------+      \--------/      +-----------------+
```

Figure 2: Distributed Quantum Computing

5.3. Secure Quantum Computing with Privacy Preservation

Secure computation with privacy preservation refers to the scenario:

1. A client node with source data delegates the computation of the source data to a remote computation node.

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, the client node could be a virtual voice-controlled home assistant device like Amazon's Alexa product. The remote computation node could be a quantum computer in the cloud. A resident as an end-user uses voice to control the home device. The home device captures voice-based commands from the end-user. Then, the home device interfaces to a home quantum terminal node (e.g., a home gateway), which interacts with the remote computation node to perform computation over the captured voice-based

commands. The home quantum terminal could be either a bare-bone quantum end-node or a full-fledged quantum computer.

In this particular case, there is no privacy concern since the source data (i.e., captured voice-based commands) will not be sent to the remote computation node which could be compromised. Protocols [Fitzsimons] for delegated quantum computing or blind quantum computation can be leveraged to realize secure delegated computation and guarantee privacy preservation simultaneously. Using delegated quantum computing protocols, the client node does not need send the source data but qubits with some measurement instructions to the remote computation node (e.g., a quantum computer).

After receiving qubits and measurement instructions, the remote computation node performs the following actions:

1. It first performs certain quantum operations on received qubits and measure them according to received measurement instructions

to generate computation results (in classic bits).

2. Then it sends the computation results back to the client node via classical channel.

3. In this process, the source data is not disclosed to the remote computation node and the privacy is preserved.

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


```
+-----------------+
|    End-User     |
|(e.g., Resident)|
+-----------------+
        ^
        | User Interface
        | (e.g., voice commands)
        V
+-----------------+
|   Home Device   |
+-----------------+
```

```
                 ^
                 | Classic
                 | Channel
                 V
        +----------------+     /--------\     +----------------+
        |                |--->( Quantum  )--->|                |
        |   Quantum      |    ( Internet )    |   Remote       |
        |   Terminal     |     \--------/     |   Computation  |
        |   Node         |                    |   Node         |
        |  (e.g., Home   |     /--------\     |   (e.g., QC    |
        |   Gateway)     |    ( Classical)    |   in Cloud)    |
        |                |<-->( Internet )<-->|                |
        +----------------+     \--------/     +----------------+
```

Figure 3: Secure Computation with Privacy Preservation

6. General Requirements

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 [Grumbling] for quantum computing. Currently, a NISQ computer can achieve fifty to hundreds of qubits with some 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-qubit machine has a total error rate which is close to the total error rate of a 7-year old two-qubit machine [Grumbling].

Although it is challenging to predict future progress of quantum technologies, some general and functional requirements on the Quantum Internet from the networking perspective, based on the above applications and use cases, are identified as follows:

1. Methods for facilitating quantum applications to interact efficiently with entanglement 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 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.

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 must be sent via classical channels.

7. Conclusion

This document provides an overview of some expected applications for the Quantum Internet, and then details selected use cases. The applications are first grouped by their usage which is a natural and easy to understand classification scheme. The applications are then 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 persons 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 specific Quantum Internet functionality required to implement the applications and uses cases described herein. To this end, a few key requirements for the Quantum Internet are specified.

8. IANA Considerations

This document requests no IANA actions.

9. Security Considerations

This document does not define an architecture nor a specific protocol for the Quantum Internet. It focuses on detailing use cases and describing typical Quantum Internet applications. However, some useful observations can be made regarding security as follows.

It has been clearly identified that once large-scale quantum computing becomes reality it will be able to theoretically break many of the public-key (i.e., asymmetric) cryptosystems currently in use because of the exponential increase of computing power with quantum computing. This would negatively affect many of the security mechanisms currently in use on the classic Internet. This has given strong impetus for starting development of new cryptographic systems that are secure against quantum computing attacks [NISTIR8240].

Paradoxically, development of a Quantum Internet will also mitigate the threats posed by quantum computing attacks against public-key cryptosystems. Specifically, the secure communication setup feature of the Quantum Internet as described in Section 5.1 will be strongly resistant to both classical and quantum computing attacks.

Finally, Section 5.3 provides a method to perform remote quantum computing while preserving the privacy of the source data.

10. Acknowledgments

The authors want to thank Mathias VAN DEN BOSSCHE, Xavier de Foy, Patrick Gelard, Wojciech Kozlowski, Rodney Van Meter, and Joseph Touch for their very useful reviews and comments to the document.

11. Informative References

[BB84] Bennett, C. and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", 1984, <http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf>.

[Cacciapuoti01] Cacciapuoti, A. and et. al., "Quantum Internet: Networking Challenges in Distributed Quantum Computing", IEEE Network, (Early Access), 2019, <https://ieeexplore.ieee.org/document/8910635>.

[Cacciapuoti02]
Cacciapuoti, A. 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://arxiv.org/abs/1907.06197>.

[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>.

[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>.

[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>.

[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>.

[Fitzi] Fitzi, M. and et. al., "A Quantum Solution to the Byzantine Agreement Problem", 2001, <https://arxiv.org/pdf/quant-ph/0107127.pdf>.

[Fitzsimons]
Fitzsimons, J., "Private Quantum Computation: An Introduction to Blind Quantum Computing and Related

Protocols", 2017,
<https://www.nature.com/articles/s41534-017-0025-3.pdf>.

[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>.

[I-D.dahlberg-ll-quantum]
Dahlberg, A., Skrzypczyk, M., and S. Wehner, "The Link Layer service in a Quantum Internet", draft-dahlberg-ll-quantum-03 (work in progress), October 2019.

[I-D.irtf-qirg-principles]
Kozlowski, W., Wehner, S., Meter, R., Rijsman, B., Cacciapuoti, A., and M. Caleffi, "Architectural Principles for a Quantum Internet", draft-irtf-qirg-principles-03 (work in progress), March 2020.

[I-D.van-meter-qirg-quantum-connection-setup]
Meter, R. and T. Matsuo, "Connection Setup in a Quantum Network", draft-van-meter-qirg-quantum-connection-setup-01 (work in progress), September 2019.

[Komar] Komar, P. and et. al., "A Quantum Network of Clocks", 2013, <https://arxiv.org/pdf/1310.6045.pdf>.

[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>.

[Preskill]
Preskill, J., "Quantum Computing in the NISQ Era and Beyond", 2018, <https://arxiv.org/pdf/1801.00862>.

[QinHao] 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>.

[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>.

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

[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>.

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

[ZhangQiang] 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>.

Authors' Addresses

Chonggang Wang
InterDigital Communications, LLC
1001 E Hector St
Conshohocken 19428
USA

Email: Chonggang.Wang@InterDigital.com

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

Email: rahmansakbar@yahoo.com

Ruidong Li
NICT
4-2-1 Nukui-Kitamachi
Koganei, Tokyo 184-8795
Japan

Email: lrd@nict.go.jp

Melchior Aelmans
Juniper Networks
Boeing Avenue 240
Schiphol-Rijk 1119 PZ
The Netherlands

Email: maelmans@juniper.net