Applications and Use Cases for the Quantum Internet

https://www.ietf.org/id/draft-irtf-qirg-quantum-internet-use-cases-15.txt

Chonggang Wang, Akbar Rahman, Ruidong Li, **Melchior Aelmans***, Kaushik Chakraborty

IETF 116, QIRG, March 27, 2023

(* Presenter)

Background

- Thank you to Rodney Van Meter and Wojciech Kozlowski for providing constructive comments and suggestions to v13/v14 of draft-irtf-qirg-quantum-internet-use-cases.
- The new v15 aims to address their comments and incorporate their suggestions.
- v15 for RGLC?

Comments on Previous v13/v14

Comments from Rodney Van Meter about v13

- **Comment #1:** [Sec. 3.2.1] “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.” – The last statement is not true……
- **Response #1:** Removed “which has been mathematically proven to be unbreakable”.

- **Comment #2:** [Sec. 3.2.3] “for the next couple of years we will have quantum computers as a cloud service” – Why limit it to the next couple of years?
- **Response #2:** Revised to “It's anticipated that quantum computers as a cloud service will become more available in future.”

- **Comment #3:** [Sec. 4.1] When talking about the bank scenario, you use the terms "source" and "destination". I'm pretty sure I've objected to this before. The end result of the key generation process is symmetric……
- **Response #3:** Removed the words “source” and “destination” from the bank scenario and other places as not needed.

Comments on Previous v13/v14

Comments from Rodney Van Meter about v13 (Cont.)

- **Comment #4:** [Sec. 4.1] In Sec 4.1, single-photon QKD is described, then after describing it the possibility of entangled QKD is brought up. I think this is confusing.
- **Response #4:** Moved “entangled QKD” down to the last bullet as suggested.

- **Comment #5:** [Sec. 4.1] Fig. 1: same thing, "source" and "destination" don't mean much here.
- **Response #5:** Removed “source“ and “destination” from Fig. 1.

- **Comment #6:** [FIG. 2] You don't need the ')' after "Mainframe".
- **Response #6:** Fixed it.
-
- **Comment #7:** [4.3] “And it generally does not need to transmit qubits among distributed parties.” - Above, you defined "transfer", I think specifically so we could use it in cases like this independent of whether the qubit is transmitted or teleported. You should use the term.
- **Response #7:** Replaced “to transmit” with “to transfer”.

Comments on Previous v13/v14

Comment from Wojciech Kozlowski on an ITU-T Document

- **Comment #1:** Please note that the ITU has released the following document: https://www.ietf.org/lib/dt/documents/LIAISON/liaison-2023-01-24-itu-t-sg-13-opsawg-ls-on-work-progress-on-quantum-key-distribution-qkd-network-in-sg13-as-of-november-2022-attachment-6.pdf. It would be nice to comment on the relationship between your document and the linked document at the upcoming meeting.
- **Response #1:** Added the following sentences to "1. Introduction" and cited the IUT-T document
  - *"It is noted that ITU-T SG13-TD158/WP3 [ITUT] briefly describes four kinds of use cases of quantum networks beyond quantum key distribution networks: quantum time synchronization use cases, quantum computing use cases, quantum random number generator use cases, and quantum communication use cases (e.g., quantum digital signatures, quantum anonymous transmission, and quantum money). This document focuses on quantum applications that have more impact on networking such as secure communication setup, secure quantum computing with privacy preservation, and distributed quantum computing; although these applications were mentioned in [ITUT], this document gives more details and derives some requirements from networking perspective."*

Next Steps

draft-irtf-qirg-quantum-internet-use-cases-15

- v15 is relatively stable now.
  - v15 addressed a few comments from Rodney Van Meter about v13.
  - v15 addressed a comment from Wojciech Kozlowski on ITU-T document.
  - No any other comments for v13/v14

- Do Chairs/QIRG think that the draft v15 is ready for RG Last Call?
  - This question was raised 2+ years ago; as a result, detailed reviews have been conducted and completed.
  - Comments from detailed reviews have been addressed in v15.