ITUWebinars

Quantum information technology

Episode #2: *Joint symposium on quantum transport technology*

28 April 2021 15:00 - 18:00 CEST

Co Organized by

IEEE Photonics Society UK & Ireland chapter   IEC   ITU

Q&A Transcript

Q1   I am a Master's student and I am currently exploring topics for my PhD. Should I consider Quantum communications? Is it safe to do a PhD or too early to decide? My major is electrical engineering with focus in wireless communications, robotics, Signal processing and AI

- *Hi there - I highly recommend it! It is certainly a safe area - lots of PhDs currently (I have three or four attached to my group for example). (**Response from Andrew Lord, BT**)*

Q2   In each node of the UK Quantum Network, are you using trustful relay? What have you done to guarantee its security?

- *So far, we are using trusted nodes. These nodes are in BT exchange buildings which are already very secure for access. We can additionally place the equipment in locked cabinets. I think trusted nodes are actually a GOOD thing - because it means there is still access to data from government / security agencies if needed. (**Response from Andrew Lord, BT**)*

Q3   Will BT work in satellite based QKD?

- *Yes. Watch this space for news on this in the coming weeks. (**Response from Andrew Lord, BT**)*

Q4   Is the scope of a standard perhaps too broad at this point as we would need to include a purpose, something tangible that might address, for example, interoperability? Even a measurement method. Thoughts?

- *DEFINITELY too broad for a single standard. A range of standards is needed and indeed these are being progressed. (**Response from Andrew Lord, BT**)*

Q5   Could you give more details on How does QKD help to make 5G more reliable?

- *Not so much about reliability. More about security. We have a 5G network which includes links to the end points e.g., cars but ALSO links from e.g., Road Side Units (RSUs) to control points - and then to a central control. This network accepts cars onto the network and runs all the control for the network - and this has to remain completely secure. So, we see QKD as helping with the 'behind the scenes' control plane for 5G. (**Response from Andrew Lord, BT**)*

Q6   How do you address the government issued statements about the insecurity of QKD, e.g., https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies?

- *In my opinion, the insecurity mainly comes from the low key rate, and that OTP encryption cannot be realized. If the key rate can be improved in the future, it may be much more secure. This is just a personal opinion, may be not accurate. (**Response from Chun-Xu Zhao, China Unicom**)*

ITUWebinars

Quantum information technology

Episode #2: *Joint symposium on quantum transport technology*

28 April 2021 15:00 - 18:00 CEST

Co Organized by

IEEE Photonics Society UK & Ireland chapter   IEC   ITU
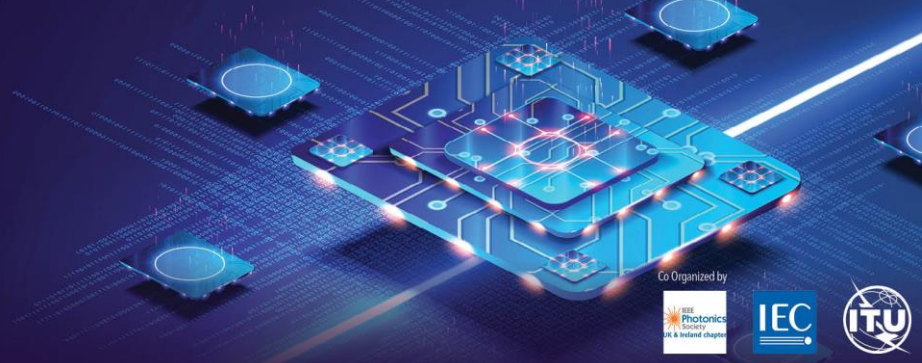
Q7   How acceptable do you expect are trusted nodes for BT and their potential customers? What are the specific requirements for protection you see?

- *Great question. We are in the process of addressing this and specifically there is a current joint piece of work being done between the Quantum Comms Hub and NCSC to resolve their remaining issues. But, for example, around authentication - we are quite clear that QKD doesn't do this and we rely on a post quantum algorithm for this part. (**Response from Andrew Lord, BT***)

Q8   How would you compare QKD and Quantum Secure Direct Communication, especially in terms of their future and applicable areas?

- *I am not familiar with QSDC. I think this is not mature for commercial use and it will take a long time to realize the tech breakthrough. (**Response from Chun-Xu Zhao, China Unicom***)

Q9   Are any carriers looking at deploying PQC/QSC over GPON?

- *If QSC stands for Quantum-secured Communication, so basically QKD (in my terminology), then I can tell you that Orange studies this!*

Q10   I may be jumping ahead here, so apologies if the question is too 'early'. We have heard from three 'national' operators talking about current state of R&D in national networks. Does the panel have any thoughts on how and when cross border quantum transport discussions should start taking place and what the key considerations (in addition to interoperability) might be?

- *Personally - I cannot see this happening at all. It is far too large a security hole.*

Q11   Is the QKD system a platform allowing flexibility of selection between QKD protocols or do we only consider one QKD protocol?

- *We want to realize the physical layer using different QKD protocol devices, and this cannot realize interchange. We just want to build one 3rd-party platform to define the interface to QKD devices and manage the key generated by different protocol QKD.*

Q12   Can you elaborate on your last bullet relative to "centralized control"?

- *We want to follow the SDN principles and plan for an SDN-like control by a centralized instance. (**Response from Matthias Gunkel, DT***)

Q13   What would be your argument against the idea where I send RNG seed generated from QRNG via PQC from node 1 to node 2 and then generate symmetric keys?

- *The issue is PQC. The point about QKD is that we are concerned that quantum computers will break all maths-based algos in time. (**Response from Andrew Lord, BT***)

Q14   Is it possible to implant PIC based QKD in parallel with PON?

- *Our DT position is that we are quite reluctant to go for co-prop with classical channels. As such we won't go for quantum channels in the same fiber as the PON fibers. (**Response from Matthias Gunkel, DT**)*

Q15   If precise channel separation/filtering is critical at the physical level, surely photonic IC's have great potential here?

- *I would expect an IC to have worse properties here - because you always compromise performance when you integrate. (**Response from Andrew Lord, BT**)*

Q16   I think filters will not be an issue but the spontaneous raman scattering (SRS) from upstream 1310nm and downstream 1490nm that kills QKD. If stacked PON over same optical distribution network is considered, there will be much more SRS!

- *Fully agree with you. That's why we, DT, do not go for co-prop. It just does not scale in case you apply this scheme together with massive DWDM. But there might be some niche applications in the last mile. (**Response from Andrew Lord, BT**)*

Q17   It is quite challenging to co-propagate QKD with stacked G-PON/10G-PON/50G PON over the same fiber. Although the QKD device self can enjoy low cost via PIC technologies.

- *PON has an inbuilt passive splitter. This is high loss (18dB for a standard splitter). The splitter could be used to randomly send different photons to different receivers though. I think the main problems would be: (i) cost of end unit, (ii) interop between PON and QKD wavelengths and how to separate them (very strong filters needed), (iii) high loss of the PON system including splitter. So - not impossible and there HAVE been publications (first one was from BT actually - in the 90s) - but hard to make practical. (**Response from Matthias Gunkel, DT**)*

Q18   The vagaries of atmosphere perhaps makes reliable communication a concern as we demonstrated in the 80s with various ground- and space-based laser weapons. The airborne laser lab may perhaps demonstrate the negative ROI for space applications. Comments?

- *Very good question. The weather problem is inevitable. But this does not affect the importance of satellite QKD. I think the main application scenarios are in the places that are not reachable by optical fibers, such as remote areas, islands and reefs, and ships. These places cannot be only relying on optical fiber QKD technology. In addition, the key can be generated in advance and then used. So I think it is possible to perform freespace QKD when the weather is good, store a certain amount of keys, and then use them. So, I think satellites still have a positive ROI. (**Response from Ji-min Nie, CAS Quantum Network**)*

Q19   The curvature of the atmosphere also makes exo-atmospheric to Earth non-trivial, so the area of viable channels may be limited.

-   *This is the case, so the development of medium and high orbit quantum satellites is an important direction. Such that the coverage could be greatly increased. Also, we can choose a ground station under good weather conditions for communication.*

-   *Yes, and also Doppler shifts play a role for the moving satellites. At the end one has to look into the complete system to find the best technical solution. But there are a number of technical solutions to the different problems regarding optimising the quantum channels.*

Q20   So, it appears that latency is not a priority?

-   *For QKD, latency is not an issue. The key can be saved for later use.*