|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | TSAG-TD424R1 |
| **TSAG** |
| **Original: English** |
| **Question(s):** | N/A | Geneva, 10-14 December 2018 |
| **TD** |
| **Source:** | Chairman, Quantum Adhoc Sessions |
| **Title:** | Minutes of the first adhoc session on Quantum |
| **Purpose:** | Information |
| **Contact:** | Arnaud TaddeiSymantec CorporationUnited States of America | Tel: +41 79 506 1129E-mail: Arnaud\_Taddei@symantec.com  |

|  |  |
| --- | --- |
| **Keywords:** | Minutes; 1st Adhoc Quantum; Tutorial |
| **Abstract:** | This document carries the minutes of the first adhoc session on Quantum. It focused on helping the team to share the same language and understanding with the help of a tutorial, question and answers and chairman’s guidance |

# Context

TSAG in its opening plenary meeting in the morning of 10th December 2018 decided to organize a TSAG - Quantum ad hoc to discuss Contribution C54 from China which proposes to create a new Focus Group on Quantum Information Technology for Networking (FG-QIT4N).

This adhoc discussion began on Tuesday 11th of December at the ITU from 8:00 to 9:30 and chaired by M. Arnaud Taddei with the support from Mrs. Xiaoya Yang, from the ITU-T Secretariat.

# Proposed Agenda

There was no written agenda when the adhoc started, but the adhoc Chairman proposed one verbally as the following:

* Welcome and opening remarks (5’)
* Agenda Approval (5’)
* Tutorial on Quantum (30’)
* Question and Answers (30’)
* How to approach contribution [C54](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T17-TSAG-C-0054) (20’)
* Any Other Business
* Closing Remarks

# Minutes

## Welcome and opening Remarks

Chairman recognizes that there could not have been any written agenda prepared before this very early morning session therefore he proposed that we could start with a tutorial on quantum in order to have a good basis for discussions, then that we could follow with questions and answers and finally that we could engage the discussion on [C54](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T17-TSAG-C-0054).

## Agenda Approval

After Canada requested the document number for the tutorial ([TD416R1](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T17-TSAG-181210-TD-GEN-0416)), the meeting agreed with the proposed agenda as in Section 2 above.

## Tutorial on Quantum

Mr Kai Chen from the University of Science and Technology of China gave an excellent tutorial on Quantum from [TD416R1](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T17-TSAG-181210-TD-GEN-0416).

This tutorial was very complete and understandable by none experts on the topic. It explained the various aspects of Quantum, its history, its potential applications, its current deployments, how it relates to other Standards Defining Organizations (SDOs), and it included a video on the benefit of Quantum.

It was finished with a round of applause.

## Questions and Answers

There were many questions to and answers from the speaker, as well as some inputs and sharing among delegates.

### Question 1 – Huawei

Huawei thanked for the excellent presentation and reminding of the historical collaboration between scientists on quantum mechanics in early 20th century, asked how we can continue this collaboration.

**Answer from Mr. Cheng:** The collaboration can be continued based on the elements at slide 44 of the presentation leading to the idea of a potential Study Group

### Question 2 – Canada

Canada thanked the speaker for this excellent presentation. Like the chairman, Canada noted that as there is significant part of the audience which are not experts of the topic, which gives a limit to this adhoc session itself.

Yet the question was about whether Quantum Safe Cryptography (QSC) includes Quantum Key Distribution (QKD) or not

**Answer from Mr. Cheng**: the answer is yes, QSC is not in conflict with QKD and includes QKD

### Question 3 – Japan

Japan thanked for this excellent presentation and confirmed that QSC includes Post Quantum Cryptography and Quantum Key Distribution. Yet Japan’s question was on a different topic. As the presentation shows a spectrum of topics from those related to SG13 and SG17, to topics such as Quantum Teleportation and Repeaters, what are the possible topics for Standardisation?

**Answer from Mr. Cheng:** In essence the topic is more than QKD and slide 44 shows some examples

### Question 4 - Canada

Canada asks if there are any production class repeaters available today in the industry?

**Answer from Mr. Cheng:** The answer is NO though slide 17 indicates how this is maturing. Mr. Cheng further clarified that Quantum can bring a lot of benefits but cannot resolve everything but has limits

### Question 5 – Switzerland

Switzerland, thanks for this presentation and clarifies that we are here to decide for a FG or not. One of the tasks of a FG is to identify areas where SG may do some work with a delay after the FG is finished. Recommendations are for products and SGs are not a research entity but rather how to define interfaces between products. Whilst quantum has left research now, yet are there any product which are mature enough and can justify engaging in standardisation. Can there be clarification on product maturity?

**Answer from Mr. Cheng:** There are examples especially in China about electric grids, cars, and other use cases.

### Question 6 – USA

USA thanks for the presentation as well as note the lack of expertise on quantum in the room. USA considers there is a need for coordination activity and we don’t want something published with wrong interoperability. As well there are terms used that are still very theoretical like Quantum Internet and that may put this field a decade away from delivering.

**Answer from Mr. Cheng:** that would be precisely goal for the work for the FG

### Question 7 – China

China shared the engagement from the EU on the field with 20 research project in 2018 and used the Chinese ‘blind people and the elephant’ metaphor to justify the need for a FG for a more broader picture of QIT beyond QKD .

### Question 8 – SG17 Chairman

SG17 Chairman thanked for the contribution and shared SG17 preference to refer to ISO/IEC JTC 1/SC 27/ WG 2 work on cryptography algorithm. He thus raised the need for coordination with SC 27/WG2.

### Question 9 – UK

UK thanks for the contribution and sees essentially two issues based on the need to not duplicate work

* Internally within the ITU where we need to coordinate between SG13, SG15 and SG17
* Externally with the ETSI and a few other SDOs

## How to approach contribution C54

Chairman offered guidance to the team on the following observations

* Chairman observes that the participants can be categorized into two groups
	+ One group is very knowledgeable of Quantum but not necessary on the ITU’s organization considerations
	+ The other group knows the ITU’s organization considerations but is not expert of Quantum
* Chairman wants to give adequate quality time for both groups to understand each other
	+ Therefore chairman announced there will be a second adhoc session tomorrow
* Chairman observes too that there are still some confusions, for example that the ETSI ISG QKD was mentioned several times but not the ETSI TC CYBER. They are very different and shows the flavour of the mathematician vs the flavour of the physician on how to resolve the problem caused by Quantum Computing to encryption.
* Chairman acknowledged that :
	+ Quantum came to ITU first with a KT contribution to SG17 which was directed to SG13 as it was more about QIT architecture and topology than security per se
	+ SG15 shouldn’t be dismissed as they rightly submitted an LS to SG13 asking about whether G.800 was followed or not
	+ SG13’s Quantum Work Item is currently under development in Q16/13. Yet a review of this Work Item shows a need for improved methodology. Indeed in its current state it will be difficult for other Study Groups (SG17 and potentially SG15) to develop cohesive Work Items on how to protect this new infrastructure or on how to have good interoperable optical relays.
	+ SG17 developed an incubation mechanism which is now hosting its 2 work items on quantum
	+ ETSI ISG QKD sent an LS ([TD406R1](https://www.itu.int/md/meetingdoc.asp?lang=en&parent=T17-TSAG-181210-TD-GEN-0406)) which opposes the creation of an FG. However the same group is happy to work on standardisation with the relevant ITU-T SGs.
* Chairman concluded that he sees the fundamental requirement is on the coordination of the work between SG13, 15, 17 and ETSI ISG QKD

Chairman proposed the following guidance

* The next adhoc will be a ‘selling exercise’ from the proponents of a Focus Group on Quantum
* He proposes to use the following questions as the methodology

**Table – Questions on FG-QIT4N proposal**

|  |  |  |
| --- | --- | --- |
| Question to answer | Why this question | Comments |
| Why a FG? | What is the value of a Focus Group on Quantum. What it would achieve that should be so unique | What is the business case for Quantum without Quantum Safe Cryptography: $1m, $10m, $1B?want to make sure that an FG is justified and is truly global and not coming from ‘just’ one country |
| Why now? | What is the compelling event that makes it relevant to start a FG now?  | Why not in a year? Or later?Is it triggered by an industry need? Market need? |
| What? | What is the scope? | Currently the proposed ToR is 80% about QKD. What are exactly the 20% other than QKD? Is slide 24 and 44 of the presentation giving the main answer?Some aspects of Quantum have matured but some others are really theoretical and very long term. We need a crisp story. |
| How? | How are you going to organize this FG?  | Any Working Group to anticipate? How to collaborate with SGs and other ITU entities? How to collaborate externally? |
| When? | What is the term of this FG?  | When does it starts and ends and on which triggers? |
| Risk of doing? | What are the risks of doing this FG?  | Are we going too far, too fast, etc.? |
| Risk of not doing? | What are the risks of not doing this FG? | Are we missing an opportunity for the Union? |
| Resources? | Who will join this FG?  | Which are the constituencies that will join to support and commit time to this FG? |
| Alignments? | What are the internal ITU and external ITU alignments? | How to not duplicate the work inside and outside the ITU? How to deal properly with ETSI ISG QKD? How to deal with current ongoing standardisation work? |
| Outcome? | What are the deliverables?  | Are they for standardisation? For WTSA? |
| Requirements? | Have we assessed the core requirements from the ITU perspective?  | How are we going to fulfil the core requirement for coordination between SG13, 15 and 17? |
| Alternatives? | Are there any other alternatives to a FG? | For example did we consider a JCA? |

Chairman hopes that:

* The second session will finish with a meeting agreement on whether we agree for a FG or not
* In case of a yes, a third adhoc session will be about drafting the final ToR and find a consensus about it before sending to the closing plenary
* In case of a no, a third adhoc session will be about finding an alternative that can be presented to the closing plenary

In addition, the meeting notes that at this stage

* Canada expressed its reserve for not to have an FG but ask for more contributions for the relevant SGs
* US agrees with the way forward proposed by adhoc Chairman
* Japan shares concerns on duplication especially with ETSI and with SG13 and 17 but could go forward if the proponents for an FG could propose to remove concerns on duplication
* Korea helped to clarify the way forward with the 2nd and 3rd adhoc (as per above)
* UK asked for a TD documenting the questions the adhoc Chairman raised as shown in the table above
* Germany supports the way forward and considers too a JCA as an alternative
* China will respect the ongoing works and alignments

## Any Other Business

There was none

## Closing Remarks

Meeting closed at 09:35.

# Conclusions

This was a very good warm up adhoc session on Quantum where the participants could benefit from a very valuable presentation. It was attended by approximately 45 delegates.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_