5-7 June. 2019
ITU QIT4N workshop
Shanghai, China

An Overview of Current Quantum Information Technology (QIT) Standardization

Wei Qi

CAS Quantum Network, Co., Ltd.

CCSA ST7 Quantum Communication and Information Technology

June 2019

The motivation of standardization

Standardization is key to QIT industry development

Driven by Science & Technology

Roots in Market Requirements

QIT Standardization Landscape

Quantum Information Technology for Networks (QIT4N)

- Analyze impacts of QIT
- Standardize QKD technology to accelerate its industrialization
- Study quantum network evolution to towards “Quantum Internet”

Quantum Computing

ISO/IEC JTC 1 INFORMATION TECHNOLOGY STANDARDS — SG2, SC7/SG1, AG

IEEE — P7130, P7131

Quantum Computing Definition, Performance Metrics & Benchmarking, etc.

Quantum Key Distribution

ITU

- SG13: QKD Network Framework
- SG17: QKD and QRNG security framework
- QKD networking related issues

ETSI World Class Standards

QKD integration into Existing Infrastructure

QKD Security Certification, Complementary Research

ISO/IEC JTC 1 INFORMATION TECHNOLOGY STANDARDS — SC 27

QKD Certification Process

Quantum Internet

IETF

QIA QUANTUM INTERNET ALLIANCE

Quantum Internet Research Group

—— existing work - - - - to be initiated

Standardization on Quantum Computing

- **2018:** JTC1 established two study groups (SG2 and SC7/SG1) on Quantum Computing
- **2019:** JTC1 establishes a new Advisory Group (AG) on Quantum Computing

- **2018:** initiated two work items on Quantum Computing Definition and Performance Metrics & Benchmarking (P7130 and P7131)

Standardization on quantum computing :

- **Still at very early stage**
- **Mainly to study the concepts, identify the standardization needs, provide performance metrics & benchmarking.**

Standardization on Quantum Key Distribution

- **2008-2018:** ETSI ISG QKD founded in 2008, and has published 6 specifications: use case, application interface, security proof, module security, optical components, etc.
- **2019~:** the progress is accelerated with 3 more specifications released: QKD vocabulary, deployment parameters, key delivery interface.

ETSI	Specification/Report	Publish date
GS QKD 002	Quantum Key Distribution (QKD); Use Cases	Jun-10
GR QKD 003	Quantum Key Distribution (QKD); Components and Internal Interfaces	Mar-18
GS QKD 004	Quantum Key Distribution (QKD); Application Interface	Dec-10
GS QKD 005	Quantum Key Distribution (QKD); Security Proofs	Dec-10
GR QKD 007	Quantum Key Distribution (QKD); Vocabulary	Dec-18
GS QKD 008	Quantum Key Distribution (QKD); QKD Module Security Specification	Dec-10
GS QKD 010	Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems	Drafting
GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems	May-16
GS QKD 012	Quantum Key Distribution (QKD) Device and Communication Channel Parameters for QKD Deployment	Feb-19
GS QKD 013	Quantum Key Distribution (QKD); Characterisation of Optical Output of QKD transmitter modules	Drafting
GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of key delivery API to Applications;	Feb-19
GS QKD 015	Quantum Key Distribution (QKD); Quantum Key Distribution Control Interface for Software Defined Networks	Drafting

Standardization on Quantum Key Distribution

- **2018:** SG 13 (future network) initiated new work item (WI) on QKD network framework; SG17(Security) initiated study on QKD network security framework and WI on quantum random number generator architecture.
- **2019**: SG13 initiated 2 WIs on QKD network architecture and key management; SG17 initiated 3 WIs on QKD network security requirements

ITU-T	Recommendation/Report	Status
Y.QKDN_FR	Framework for Networks to supporting Quantum Key Distribution	Drafting
Y.QKDN_Arch	Functional architecture of the Quantum Key Distribution network	Drafting
Y.QKDN_KM	Key management for Quantum Key Distribution network	Drafting
X.qrng-a	Quantum Noise Random Number Generator Architecture	Drafting
X.sec_QKDN_ov	Security Requirements for QKD Networks - Overview	Drafting
X.sec_QKDN_km	Security Requirements for QKD Networks - Key Management	Drafting
X.cf_QKDN	The use of cryptographic functions on a key generated by a Quantum Key Distribution networks	Drafting
TR.sec_QKD	Security framework for Quantum Key Distribution in Telecom network	Drafting

Standardization on Quantum Key Distribution

- **2017:** The study item "Security requirements, test and evaluation methods for quantum key distribution" was initiated
- **2019:** Study period was finished and new work item ISO/IEC 23837 (Part 1&2) was approved and initiated

ISO/IEC	Standard/Report	Status
Study Period	Security requirements, test and evaluation methods for quantum key distribution	Finished
ISO/IEC 23837-1	Security requirements, test and evaluation methods for quantum key distribution Part 1: requirements	Ongoing
ISO/IEC 23837-2	Security requirements, test and evaluation methods for quantum key distribution Part 2: test and evaluation methods	Ongoing

Standardization on Quantum Key Distribution

- QKD has become a hot topic for international SDOs
- Some of the most important issues have not been resolved:
  - QKD network interoperability, QKD security certification, etc
- Further coordination and collaboration are needed to improve efficiency

Standardization on “Quantum Internet”

- **2018~:** Quantum Internet Research Group(QIRG) was established; 4 documents are drafting; a simulator for developing quantum internet software(SimulaQron) was released

IETF	Internet-Drafts	Status
draft-irtf-qirg-principles-00	Architectural Principles for a Quantum Internet	I-D Exists IRTF stream
draft-dahlberg-ll-quantum-02	The Link Layer service in a Quantum Internet	I-D Exists
draft-kaws-qirg-advent-03	Advertising Entanglement Capabilities in Quantum Networks	I-D Exists
draft-van-meter-qirg-quantum-connection-setup-00	Connection Setup in a Quantum Network	I-D Exists

- **A good example for research-oriented standardization activity**
- **Helpful to promote the development of quantum network technology and potential applications**

Standardization activities within China

- **2017~:** China Communications Standards Association (CCSA) established ST7 on Quantum Communication; 25 work/study items were conducted; 6 study reports have been finished: QKD network architecture, QKD security issues, functional test method, co-fiber transmission, components and module requirements, QRNG.

No.	Standard/Report Name	Status
1	Quantum Communication Terminologies and Definitions	Drafting
2	Quantum Secure Communication application scenario and requirements	Drafting
3	Quantum Key Distribution (QKD) application interface	Drafting
4	Technical requirements for quantum key distribution (QKD) systems Part I: Decoy-state BB84	Drafting
5	Test methods of optical quantum key distribution (QKD) system	Drafting
6	Study on Quantum secure communication network architecture	Finished
7	Study on security issues of Quantum Key Distribution	Finished
8	Study on test and evaluation of Quantum Secure Communication System	Finished
9	Study on the Co-Fiber Transmission of Quantum Key Distribution and Classic Optical Communication Systems	Finished
10	Study on Generating and Testing method of Quantum Random Number	Finished
11	Study on quantum key distribution key components and modules technical requirements	Finished
12	Study on Quantum Secure Communication Network Management	Drafting
13	Study on CV-QKD technique	Drafting

No.	Standard/Report Name	Status
14	Study on software defined QKD network	Drafting
15	Study on trusted relay node in QKD network	Drafting
16	Technical Specification of WDM Systems with the Support of Quantum Key Distribution	Drafting
17	Quantum Secure Communication Network Architecture	Drafting
18	Technical Requirements of Co-Fiber Transmission System for Quantum Key Distribution and Classic Optical Communication	Drafting
19	Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 1: optical source	Drafting
20	Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 2: Single photon detector	Drafting
21	Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 3: Quantum random number generator(QRNG)	Drafting
22	Study on Quantum Secure Communication Networking Key Technologies	Drafting
23	Study on Freespace Quantum Secure Communication Technology	Drafting
24	Requirements of encrypted data carried in MPLS PW in quantum secure communication network	Drafting
25	Study on optimization protocol based on decoy state method	Drafting

Standardization activities within China

- **2016:** China Cryptography Standardization Technical Committee (CSTC) have initiated 5 work/study items on decoy state BB84 QKD technical and test specification

1	Research on technical specification of network cryptography machine based on quantum key distribution
2	Research on the framework of cryptographic communication technology based on quantum key distribution
3	Research on the framework of quantum secure communication test methods
4	Technical specification for decoy state BB84 quantum key distribution
5	Test specification for decoy state BB84 quantum key distribution

- **2015:** China information security standardization technical committee (CSTC) have initiated study of quantum-secured communication network specifications.

- **2019:** China national standardization technical committee on **quantum computing and metrology** was established

Considerations to future work

- Build more open platform to bring together global experts and strengthen cooperation
- Identify real commercial market requirements, develop practical standards to support industry growth
- Leverage the global influence of ITU, attract worldwide forces to promote the standardization of QIT

Thank you !
Q&A