Standardization of quantum cryptography in ITU-T and ISO/IEC

Hao Qin*
CAS Quantum Network Co., Ltd.

*qinhao@casquantumnet.com
Quantum key distribution: From concepts to applications

- Quantum key distribution (QKD)
- Information theoretic security based on quantum physics

First QKD experiment in IBM 1992

QKD commercial products

IDQ, QCTEK, Toshiba, QRate, XT etc.

QKD Network (QKDN)

EU SECOQC

Tokyo Network

Beijing-Shanghai Backbone

QKD satellite
International Standards Development Organizations (SDOs)

- **International Organization for Standardization (ISO)**
  - Non-Governmental Organization, founded in 1947
  - An international standard-setting body composed of representatives from various national standards organizations
  - Promotes worldwide proprietary, industrial, and commercial standards

- **International Electro-technical Commission (IEC)**
  - Not-for-profit, quasi-governmental organization, founded in 1906
  - International standards for all electrical, electronic and related technologies, known as "electrotechnology".

- **International Telecommunication Union (ITU)**
  - Originally the International Telegraph Union created in 1865
  - A specialized agency of the United Nations for information and communication technologies
  - The oldest global international organization
  - The first international standards organization
Standardization activities in SDOs

- **European Telecommunications Standards Institute (ETSI)**
  - Standardization activities of QKD since 2008
  - All aspects of QKD: 8 specifications, 2 white papers

- **ISO/IEC JTC1**
  - Information technology
  - SC 27 WG 3: QKD implementation security
  - SC 27 WG 2: Post quantum cryptography (PQC)
  - WG 14: Quantum computing

- **International Telecommunication Union (ITU)**
  - SG 13: QKDN network aspects
  - SG 17: QKDN security aspects
  - FG QIT4N WG2: QKDN terminology, use cases, protocols, transport etc (Pre-standardization)
Standardization aspects in QKDN based on trusted nodes

FG QIT4N: terminology

FG QIT4N: use cases

FG QIT4N: Classical protocols

FG QIT4N: QKD protocols, transport technology

* Conceptual structures of a QKDN and a user network in Rec. ITU-T Y.3800 (10/2019)

ITU-T SG 13: Network arch. Functions; QoS

ITU-T SG 17: Security requirements

ISO/IEC: Test and certification

- Standards
- Pre-study
Standardization activities in ISO/IEC JTC1 SC27 WG3

- **ISO/IEC 23837**: Security requirements, test and evaluation methods for quantum key distribution
  - Part 1: Requirements
  - Part 2: Test and evaluation methods

- Work item initiated in 2018 with one year preliminary study in 2017, currently under development

- Address QKD implementation security issues

- High-level framework for the security evaluation of QKD module under the Common Criteria (CC) (ISO/IEC 15408) framework

https://www.iso.org/standard/77097.html
https://www.iso.org/standard/77309.html

- A baseline of Security Functional Requirements (SFRs), and relevant evaluation activities (EAs) for SFRs and SARs, and serve as a basis for developing relevant PPs/STs
- EAs for functional conformance test and vulnerability assessment (up to EAL5+AVA_VAN.5)
Standardization activities in ISO/IEC JTC1 SC27 WG3

ISO/IEC 23837-1: Security requirements

ISO/IEC 23837-2: Test and evaluation methods
Standardization activities in ITU-T SG 13

Study group 13: Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures

<table>
<thead>
<tr>
<th>#</th>
<th>Work item</th>
<th>Name</th>
<th>Timing</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y.3800</td>
<td>Framework for Networks to supporting Quantum Key Distribution</td>
<td>Published 2019-10</td>
<td>Q16</td>
</tr>
<tr>
<td>2</td>
<td>Y.3801</td>
<td>Functional requirement of the Quantum Key Distribution network</td>
<td>Published 2020-05</td>
<td>Q16</td>
</tr>
<tr>
<td>3</td>
<td>Y.3802</td>
<td>Functional architecture of the Quantum Key Distribution network</td>
<td>Consented 2020-07</td>
<td>Q16</td>
</tr>
<tr>
<td>4</td>
<td>Y.3803</td>
<td>Key management for Quantum Key Distribution network</td>
<td>Consented 2020-07</td>
<td>Q16</td>
</tr>
<tr>
<td>5</td>
<td>Y.3804</td>
<td>Control and Management for Quantum Key Distribution Networks</td>
<td>Consented 2020-07</td>
<td>Q16</td>
</tr>
<tr>
<td>6</td>
<td>Y.QKDN_sdnc</td>
<td>Software Defined Network Control for Quantum Key Distribution Networks</td>
<td>2021-09</td>
<td>Q16</td>
</tr>
<tr>
<td>7</td>
<td>Y.QKDN_bm</td>
<td>Business role-based models in Quantum Key Distribution Network</td>
<td>2021-03</td>
<td>Q16</td>
</tr>
<tr>
<td>8</td>
<td>Y.QKDN_frint</td>
<td>Framework for integration of QKDN and secure network infrastructures</td>
<td>2021-07</td>
<td>Q16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Work item</th>
<th>Name</th>
<th>Timing</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Y.QKDN-qos-req</td>
<td>Requirements for QoS Assurance of the Quantum Key Distribution Network</td>
<td>2021-10</td>
<td>Q6</td>
</tr>
<tr>
<td>10</td>
<td>Y.QKDN-qos-gen</td>
<td>General Aspects of QoS (Quality of Service) on the Quantum Key Distribution Network</td>
<td>2021-10</td>
<td>Q6</td>
</tr>
<tr>
<td>11</td>
<td>Y.QKDN-qos-fa</td>
<td>Functional architecture of QoS assurance for quantum key distribution networks</td>
<td>2021-12</td>
<td>Q6</td>
</tr>
<tr>
<td>12</td>
<td>Y.QKDN-qos-ml-req</td>
<td>Requirements of machine learning based QoS Assurance for quantum key distribution networks</td>
<td>2022-07</td>
<td>Q6</td>
</tr>
</tbody>
</table>

Q6: Quality of service (QoS) aspects including IMT-2020 networks
Q16: Knowledge-centric trustworthy networking and services

### Standardization activities in ITU-T SG 17

#### Study Group 17: Security

<table>
<thead>
<tr>
<th>#</th>
<th>Work item</th>
<th>Name</th>
<th>Topic</th>
<th>Timing</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>X.1702</td>
<td>Quantum Noise Random Number Generator Architecture</td>
<td>QRNG</td>
<td>Published 2019-11</td>
<td>Q4(Cybers ecurity )</td>
</tr>
<tr>
<td>2</td>
<td>X.sec_QKDN _ov</td>
<td>Security Requirements for QKD Networks – Overview</td>
<td>Security Req.</td>
<td>2020-08</td>
<td>Q4</td>
</tr>
<tr>
<td>3</td>
<td>X.sec_QKDN _km</td>
<td>Security Requirements for QKD Networks - Key Management</td>
<td>Security Req.</td>
<td>2020-08</td>
<td>Q4</td>
</tr>
<tr>
<td>4</td>
<td>X.cf_QKDN</td>
<td>Key combination and confidential key supply for quantum key distribution networks</td>
<td>Security app.</td>
<td>2020-08</td>
<td>Q4</td>
</tr>
<tr>
<td>5</td>
<td>X.sec_QKDN _tn</td>
<td>Security requirements for Quantum Key Distribution Networks-Trusted node</td>
<td>Security Req.</td>
<td>2021-03</td>
<td>Q4</td>
</tr>
<tr>
<td>6</td>
<td>TR.sec_QKD</td>
<td><strong>Tech. Report</strong>: Security considerations for Quantum Key Distribution network</td>
<td>Security study</td>
<td>Published 2020-03</td>
<td>Q4</td>
</tr>
</tbody>
</table>

PRE-standardization activities in ITU-T QIT4N

ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N)

- Pre-study and pre-standardization
  - Gap analysis, status review, standardization analysis, future suggestions
  - Technical reports with NO normative contents
- Open platform for academic, industry, governments etc.
  - Established in 2019-10
  - 1 onsite meeting in Jinan, China; 4 E-meetings
- WG1: Network aspects of QIT
- WG2: QKD network

https://www.itu.int/en/ITUT/focusgroups/qit4n/Pages/default.aspx

FG QIT4N WG2:QKDN

<table>
<thead>
<tr>
<th>Sub-group</th>
<th>Name</th>
<th>Current Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>D2.1</td>
<td>QIT4N terminology part 2: quantum key distribution network</td>
<td>QIT4N-O-048</td>
</tr>
<tr>
<td>D2.2</td>
<td>Technical report on the QIT4N use case part 2: quantum key distribution network</td>
<td>QIT4N-O-049</td>
</tr>
<tr>
<td>D2.3</td>
<td>Technical report on QKDN protocols</td>
<td>QIT4N-O-050&amp;51</td>
</tr>
<tr>
<td>D2.4</td>
<td>Technical report on QKDN transport technologies</td>
<td>QIT4N-O-052</td>
</tr>
<tr>
<td>D2.5</td>
<td>Technical report on QIT4N standardization outlook and technology maturity part 2: quantum key distribution network</td>
<td>QIT4N-O-053</td>
</tr>
</tbody>
</table>
Participations

- Main contributors from China, Japan, Korea, Switzerland, UK, US etc.

- Restricted to experts from each country’s national body channel

- Study groups: Membership based
  Activities in study groups with different topics

- Focus group: open for everyone
  Free of charge, new comer friendly, flexibility, wide range of topics
  Liaison channels among different SDOs
Gap analysis and possible future works

Ongoing studies in ISO/IEC; ITU-T study groups, FG-QIT4N
Potential future studies in SDOs

Quantum Key Distribution Network

- QKD module security (ISO/IEC)
- Security aspects (ITU SG 17)
- Network aspects (ITU SG 13)
- Protocol and test methods
- Transport technologies
- Applications
- Network operation aspects
- Other possible directions
Thanks.