Towards large-scale quantum key distribution network and its applications

Hao Qin
CAS Quantum Network Co., Ltd.
Email: qinhao@casquantumnet.com
Quantum Key Distribution (QKD): from theory to practice

1984 Bennett & Brassard Invent BB84 Protocol

1989 IBM: first lab test for quantum information transmission (32 cm)

2003 US: DARPA QKD network with 10 nodes

2004 EU: SECOQC network initiated, finished at 2008

2005: Decoy-state solution proposed to extend QKD to more than 100KM*

2008 Hefei 3 nodes telephone network (20KM)
- Hefei 5 nodes full-pass QKD network
- Geneva QKD network
- Madrid QKD network

2009 JP: Tokyo QKD network

2010 Hefei QKD metro network (46 nodes)

2012 Jinan metro QKD network (56 nodes)
- Beijing-shanghai trunk initiated

2013 Global large scale QKD network plans accelerating

2016: “Micius” quantum satellite launched

Global satellite QKD projects initiated

Global QKD network projects

- DARPA QUANTUM NETWORK, BBN Technology (2007)
- EU SECOQC QKD network, 10.1002/sec.13 (2008)
- Tokyo QKD network, OE.19.010387 (2011)
- SwissQuantum QKD network, NJP 13(12), 123001 (2011)

AND SO ON......
QKD network: Three layers architecture

Application layer

Network management & function layer

QKD link layer

QKD-based SSL, IPSEC, …
Large-scale QKD network as infrastructures

- **Goal:** Provide information security services through scalable, service-oriented and cost-efficient QKD networks in wide area.
- **Support various services and applications based on QKD network.**
- **Build and operate the QKD network.**

Technology/standard requirements for QKD link and network layers.

---

ITU QIT4N Workshop 2019

[C. H. Bennett & G. Brassard, BB84 protocol (1984)]
Technology requirements: QKD link layer

- Solve the key distribution problem
  - Security based on quantum physics: Information theoretic security
  - Point-to-point symmetric key establishment: Rate-loss trade-off

- Not rely on single QKD protocol!
  - Well studied and mature enough: Complete security proof; robust performance in practice; efficient key rate output etc.
  - Discrete Variable (DV) QKD: BB84 with decoy
  - Continuous Variable (CV) QKD: GG02
  - Polarization and phase encoding etc.

- Open for new protocols:
  - Measurement device independent (MDI) QKD
    - HK Lo et al., PRL 108, 130503 (2012)
  - Twin filed (TF)/Phase matching (PM) QKD

ITU QIT4N Workshop 2019
Technology requirements: Network layer

• Trusted node  • Optical switch

- Key materials relay: XOR operations
- Key resources or user key protection
- Protection on the trusted node
- Working with optical switches
- Quantum relay is currently not available in practice

ITU QIT4N Workshop 2019

• Wavelength Division Multiplexing (WDM)

- Integration of QKD in optical WDM networks
- Quantum signals share a same fiber with classical signals
- Largely reduce fiber resources and cost

Technology requirements: Network layer

QKD network control & management functions

• **QKM**: Quantum key exchange, storage, use
• **Q-AuC**: Node Register and Authentication
• **Q-PCRF**: QoS Policy and Charging Rules control

• **Q-MN**: Routing and Resource Management, e.g., load balancing

• **Interoperability**: Support multi-vendor interoperability for both QKD and network management devices
• **Scalability**: Flexible and economic network expansion, flexible network topology for wide-area coverage

CAS Quantum Network 2018
Standard requirements: QKD link layer

QKD basis
- Definition/Vocabulary
- Protocols
- Components
- Characterization: transmitter & receiver
- Classical post processing etc.

QKD security
- Security proof
- Module Security Specification
- Security statement:
  - Definition, assumptions, requirements
- Security certification & evaluation of QKD
- Security analysis & Test methods of QKD

TABLE 1: Summary of potential security issues in QKD systems.

<table>
<thead>
<tr>
<th>Potential security issue</th>
<th>C</th>
<th>Q</th>
<th>Target component</th>
<th>Brief description</th>
<th>Requirements for complete analysis</th>
<th>Lab testing, evaluation needed?</th>
<th>Risk evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CX Q1-5.7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>CX Q1-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>CX Q1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>C0 Q2.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>CX Q4-5.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>medium</td>
<td></td>
</tr>
<tr>
<td>CX Q1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>high</td>
<td></td>
</tr>
<tr>
<td>CX Q1-5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>insufficient information</td>
<td></td>
</tr>
<tr>
<td>CX Q1-9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>low</td>
<td></td>
</tr>
<tr>
<td>CX Q1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>medium</td>
<td></td>
</tr>
<tr>
<td>CX Q4.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
<td>low</td>
<td></td>
</tr>
</tbody>
</table>

- Session 3A Technology “Security analysis for QKD”
- Session 6A Global Standardization Progress” QKD standardization in ISO/IEC JTC 1/SC 27”
Standard requirements: Network layer

- **Network basis**
  - Network architecture
  - Network component function
  - Software defined network (SDN)
  - Trusted node key relay
  - Key management
  - Application Interface
  - Coexistence of quantum and classical channels

- **Network security requirements**
  - Overall security requirement
  - Link security requirement
  - Key management security requirement
  - Applications & services security requirement
  - Trusted relay protection
QKD related standards in China

- Most of the QKD standard topics are also considered in China.
- Chinese growing QKD industries push forward standard research activities.

In Jun. 2017, CCSA established the 7th Special Task Group (ST7) focused on QKD-based Quantum Secure Communication (QSC).

In 2017, cryptography standardization technical committee started the QKD standards research focusing on security requirements and test methods.

Most of the QKD standard topics are also considered in China.

Chinese growing QKD industries push forward standard research activities.
Satellite-ground integrated QKD networks in China

- 2000 km Beijing-to-Shanghai backbone (2013~2017)
- World’s first quantum satellite “Micius” (2016~)
- Hierarchical: metropolitan access network, wide-area fiber backbone network and satellite network
- Scalable based on trusted relay and optical switch
- Support various topology and applications, e.g., ITS voice, AES encrypted video, IPSEC VPN, etc.
QKD applications in financial sectors

- QKD network-based bank data transfer and data center backup in ICBC
- Security enhancement of business data transfer

- Online banking and transactions for enterprise users with QKD security enhancement in Bank of Communications
QKD trail applications in other domain

- **Customs ERP network system**
  - Using quantum secure communication to improve the information security level of import and export enterprise network access to customs intranet and ERP data center. The project is planned to be promoted in the national customs system, covering more than 1.6 million import and export enterprises.

- **QKD network for Court system**
  - Supreme Court and Local High Court achieve cross-province quantum encrypted data transmission through "Beijing-Shanghai quantum backbone line". High Court uses offline quantum key to ensure safe applications of the court business system in the Internet environment.

ITU QIT4N Workshop 2019
National quantum secure communication backbone network

• From 2017 to 2025, we will build a national wide-area quantum communication backbone network "Satellite-ground integration, five-horizontal and six-vertical lines".

• With a total length of about 35,000 kilometers, it covers large and medium-sized cities across the country and connects to major data centers.

• Coverage extends to oversea regions, services for national strategies and secure communications with foreign institutions.
Global satellite-based QKD network

- [Liao et al., PRL 120, 030501 (2018)]
  - Intercontinental QKD with “Micius” quantum satellite
  - AES encrypted video call using quantum keys from QKD
  - Feasibility demo: Satellite as a trusted relay

- Global Satellite-ground integrated QKD networks
- Ambitious and challenges but feasible....
- Coming in near future!
Thanks!

Q&A