Development and evaluation of QKD-based secure communication in China

China Academy of Information and Communication Technology (CAICT)
Wen-yu Zhao
Email: zhaowenyu@caict.ac.cn
6 June 2019
Outline

- Background
- Status of QKD-based secure communication (QSC) in China
- Test and evaluation of QSC
- Conclusion
Quantum information technology (QIT) overview

Quantum communication: Use quantum superposition or entanglement to transmit key or information, providing information theory security guarantees based on the principle of quantum mechanics.

Quantum computing: Use quantum bits to realize information coding, storage, and processing through the controlled evolution of quantum states, which provides superior computing and information processing capability.

Quantum sensing: Manipulate and detect the particle quantum state to measure various physical quantities such as gravity, magnetic field, and time, which provides advantages in accuracy, sensitivity, and stability.
Prospects of future QIT application and influence

Fundamental problems and bottlenecks of quantum physics are control factors for the practical application of quantum information technology.

- Universal quantum computer, quantum computing software and application
- Quantum information nodes networking, quantum internet
- Quantum computing prototype, quantum simulator
- Quantum key Distribution, Quantum secure communication
- Quantum satellite, wide-area quantum communication network and application
- Optical/atomic clock, quantum gravimeter, magnetometer, gyro, imager...
- Quantum sensor chip and integrated system

Short term <5 years | Mid term ~10 years | Long term >10 years

Estimated application time
Quantum teleportation can realize direct transmission of quantum information, is still in the stage of experimental research. Quantum key distribution can share keys between the two parties and use the keys to encrypt information, has entered the preliminary practical stage.
QKD-based secure communication

- Quantum key distribution (QKD), typically Decoyed-BB84, can provide theoretically unconditional security of key sharing based on the laws of quantum physics only.
- QKD based symmetric cryptography, which can be referred as quantum secure communication (QSC), is one of the promising information security solutions in the post-quantum era.

**Symmetric Cryptography**

**Key Management**

**Quantum Key Distribution**

- ATE: auxiliary transmission equipment
- DC: quantum channel
- EAI: encryption application interface
- ETC: encrypted transmission channel
- KMC: key manage channel
- KMI: key manage interface
- NMC: network manage channel
- QC: quantum channel
- QEA: quantum encryption application
- QKM: quantum key management
- SC: synchronization channel
QKD-based QSC demo and trial network in China

2004, Beijing-Tianjin 125 km, the first quantum cryptography.

2013, Jinan 50-node Quantum Secure Communication Network.

2016, quantum secure communication “Beijing-Shanghai backbone line”.

2007, 4-node Beijing Netcom network of quantum cryptography.

2012, Xinhua News Agency financial information quantum secret communication line.


2008, Hefei 3-node all-pass quantum secure telephone.

2011, Hefei and Wuhu metropolitan quantum secure communication network.

2018, 1st phase of the “national wide-area quantum secure communication backbone network”.

First phase of “national wide-area quantum secure communication backbone network “project
QSC industry status in China

Information Security Application
Hefei, Jinan, Wuhan...

Network Construction & Operation

System Research & Development

Academic Research & Experiment
USTC, THU, SXU, NJU, BUPT, PKU, SJTU, JN1Q, SCNU, ...

Government
Financial
Infrastructure
Data center

China ComService

State Grid

Bank of Communications

Alibaba Cloud

Tencent Cloud...
The role of CAICT in QSC industry

- Frontier scientific research
- Hero experiments
- Demonstration application
- Industrialization research
- Test and evaluation
- Standardization
- Industrial application
- Network deployment
- Business operation

Quantum Academia

ICT Industry
Test and evaluation framework of QSC system

- Test and evaluation is indispensable step for QKD-based QSC technology to get industrial application and large scale deployment.
- Test evaluation framework of QKD/QSC system function and performance has been established. Requirements of QSC system and network verification have been considered.

Diagram showing the framework with nodes such as QSC, QKD, QKM, and QEA. The framework includes interface/module, system, management, and encryption with specific requirements like key generation rate, protocol consistency, key manage, encryption function, and encryption performance.

Reference points:
- Sc: Transmitter clock signal
- Sq: Transmitter quantum signal
- Ss: Transmitter synchronization signal
- St: Transmitter test signal
- Rc: Receiver clock signal
- Ro: Receiver SPD output signal
- Rq: Receiver quantum signal
- Rs: Receiver synchronization signal
Quantum key distribution system evaluation

- SPD in QKD receiver is directly related to system key rate and transmission performance. The detecting probability ($\eta$), after-pulse probability, dark count, dead time, and detection response of SPD can be measured by a comprehensive test environment.

- G.652D SSMF and VOA are used to test QKD system key rate under different channel loss. BB84 protocol consistency can be checked by distillation channel packet capture analysis.

<table>
<thead>
<tr>
<th>QKD system test projects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transmitter</strong></td>
</tr>
<tr>
<td>Quantum channel time domain: frequency, pulse width, ...</td>
</tr>
<tr>
<td>Quantum channel frequency domain: wavelength, ...</td>
</tr>
<tr>
<td>Quantum channel mean-photon-number</td>
</tr>
<tr>
<td>Synchronization channel time domain: frequency, pulse width, ...</td>
</tr>
<tr>
<td>Synchronization channel frequency domain: wavelength, ...</td>
</tr>
<tr>
<td>QRNG Randomness</td>
</tr>
<tr>
<td><strong>Receiver</strong></td>
</tr>
<tr>
<td>Gated signal time domain: frequency, jitter, ...</td>
</tr>
<tr>
<td>SPD dark count</td>
</tr>
<tr>
<td>SPD detection efficiency</td>
</tr>
<tr>
<td>SPD after-pulse-probability</td>
</tr>
<tr>
<td>SPD dead time</td>
</tr>
<tr>
<td>Synchronization channel receiving sensitivity</td>
</tr>
<tr>
<td><strong>System</strong></td>
</tr>
<tr>
<td>Key generation rate and relation with channel loss</td>
</tr>
<tr>
<td>Key consistency and randomness</td>
</tr>
<tr>
<td>BB84 protocol consistency</td>
</tr>
<tr>
<td>System startup time</td>
</tr>
<tr>
<td>System redundancy protection</td>
</tr>
<tr>
<td>System long-term work stability</td>
</tr>
<tr>
<td>System reliability under environmental change</td>
</tr>
</tbody>
</table>
Quantum secure communication system evaluation

- Quantum encryption equipment can be VPN, IP router, OTN, or other kind of data transmission equipment which support symmetric encryption and quantum key source input. Several encryption algorithms and check algorithms can be supported, and encrypted channel capacity is various.

- Traditional IKE key backup for the absence of quantum key is also supported. Temperature and humidity variation test are performed to verify system reliability.

<table>
<thead>
<tr>
<th>QSC system test projects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auxiliary transmission equipment</strong></td>
</tr>
<tr>
<td>WDM: inser loss, wavelength, spectrum, isolation, …</td>
</tr>
<tr>
<td>Optical lane switch: inser loss, wavelength, switching, …</td>
</tr>
<tr>
<td><strong>Key management equipment</strong></td>
</tr>
<tr>
<td>Device management function,</td>
</tr>
<tr>
<td>Key management function</td>
</tr>
<tr>
<td>Networking management function</td>
</tr>
<tr>
<td><strong>Encryption application equipment</strong></td>
</tr>
<tr>
<td>Encryption algorithms and functions</td>
</tr>
<tr>
<td>Encryption service performance</td>
</tr>
<tr>
<td>Key source backup and switching function</td>
</tr>
<tr>
<td>Encryption service redundancy protection</td>
</tr>
<tr>
<td><strong>System</strong></td>
</tr>
<tr>
<td>System startup time</td>
</tr>
<tr>
<td>System redundancy protection</td>
</tr>
<tr>
<td>System long-term work stability</td>
</tr>
<tr>
<td>System reliability under environmental change</td>
</tr>
<tr>
<td>Clock synchronization function</td>
</tr>
</tbody>
</table>
Typical technical challenges for future QSC application

- **Practical Security**
  - Security proof of practical QKD system and protecting solutions against various component loopholes, system side-channels, and attack schemes are under study. The practical QKD and QSC system security test evaluation and standardization are still open questions.

- **Interoperability**
  - Because of the point-to-point nature of QKD, the interoperability of QSC network can be considered in the QKM layer. Consistent understanding of key relay strategy, networking interface and management solutions are the prerequisite for further standardization.

- **Engineering**
  - QSC system still has some room for improvement in terms of equipment performance, engineering level, standardization degree, stability and reliability, operation and maintenance support capability. It is necessary to further make improvement and test verification.
Conclusion

- Quantum information technology (QIT) is becoming a hot topic in ICT, QKD-based QSC is one of the promising information security solutions in the post-quantum era.

- QSC networks have been constructed in several cities, wide-area network project is under construction, industrial chain will get further development.

- Function and performance test evaluation framework of QSC system and network have been established, and some critical parameters of QKD and QSC systems are evaluated by CAICT as a third-party.

- There are still some technical challenges and problems for QSC application need to be solved, including practical security, interoperability, and more robust engineering.
Thanks for your attention!