The Chinese QKD networks

Hong Xiang
Chongqing University
xianghong@cqu.edu.cn

Zheng-Fu Han
University of Science and Technology of China
zfhan@ustc.edu.cn

3rd ETSI Quantum Safe Cryptography Workshop
Seoul, Korea
5-7 October, 2015
Who was the first QKD guy in China?

Overview of QKD networks in China

Advanced QKD research in China

Space...the final frontier
First-mover in China

- 20 years ago, Professor Ling-An Wu implemented the first “concept-proof” of QKD experiment in China, with few undergraduate students, and with less than 100 RMB budget.
- 20 years passed China has one of largest QKD network projects in the world and over billions R&D budgets.
- We made some progress but there are still lots of things to catch up.
The QKD network in 2007, Beijing

Beijing four users QKD network (2007)

- The second field test network in the world
- The first full-time all-pass WKD network
- The first field test for the decoy states in fiber lines.

Characteristic

- Full-time all-pass (any time, any user)
- Can be realized in commercial WDM
- Any two users add-in just two WDMs
- Symmetry network, Automatic addressing
- Good scalability
The QKD network in 2010, Wuhu City

- Backbone Network —— Quantum Router
- Subnet —— Switch Router
- dual-network integration —— Trust Relay
The QKD network in Wuhu City

- Quantum router
- Quantum switch

The QKD network in Wuhu city employed with both quantum routers and quantum switches.

Fang-Xing Xu et al., Chin. Sci. Bull. 54, 2991 (2009)
The QKD network in Wuhu City

Wavelength-saving quantum key distribution network:
Direction as a signal exchange dimension

Hefei-Chaohu-Wuhu QKD wide area network

Shuang Wang et al., Opt Express, 22, 21739 (2014)
Hefei-Chaohu-Wuhu QKD wide area network

- The first cross-city WAN
- 150km length crossing Yangzi River Bridge (think about the case that when trains pass through...)
- Stably operating over 5000 hours
Hefei-Chaohu-Wuhu QKD wide area network

Transmitter and receiver sectional device

Transmitter and receiver all-in-one device

3.5U Standard telecom case
Hefei-Chaohu-Wuhu QKD wide area network

**Network topological structure**
Hefei-Chaohu-Wuhu QKD wide area network

The final test: Error Rate

<table>
<thead>
<tr>
<th></th>
<th>R1</th>
<th>R2</th>
<th>R3</th>
<th>R4</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>0.97%</td>
<td>0.85%</td>
<td>0.70%</td>
<td>1.12%</td>
</tr>
<tr>
<td>T2</td>
<td>0.48%</td>
<td>1.02%</td>
<td>0.53%</td>
<td>1.07%</td>
</tr>
<tr>
<td>T3</td>
<td>0.86%</td>
<td>0.91%</td>
<td>1.09%</td>
<td>0.78%</td>
</tr>
<tr>
<td>T4</td>
<td>0.56%</td>
<td>0.62%</td>
<td>0.49%</td>
<td>0.67%</td>
</tr>
</tbody>
</table>

Hefei-Chaohu-Wuhu QKD wide area network

Fiber Length: 85.1km
Attenuation: 18.4dB
Quantum Backbone

Based on trustable relay, setting up “Quantum Backbone”
Quantum Backbone

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes
- 31 fiber links
- Metropolitan networks
- Existing: Hefei, Jinan
- New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC
Ground test of satellite-based photon transmission

- Single photon transmission between satellite and ground at the distance of 400km (2009)
- Direct and full-scale experimental verifications towards ground-satellite QKD

China’s Quantum Experiments Plan in Space

- High-rate QKD between satellite and ground
- Quantum entanglement distribution from satellite, test of Bell’s inequality over macro-scale
- Quantum teleportation between satellite and ground
Qasky Quantum Science and Technology Co. Ltd.

**QKD Terminal:**
- Decoy-state BB84 protocol;
- Single photon emission and receiving;
- High speed;
- Robust;
- International patents held.

**QKD exchange & Router:**
- Important devices in QKD networks;
- Full-time & all-pass devices;
- Own intellectual property rights owned and patents held.

**Quantum VPN:**
- QKD supported;
- High secure key refresh rate;
- Compatible for traditional encryption;
- Compatible for current networks.

**Single photon detector:**
- Important devices in QKD networks;
- Not only for QKD;
- Single photon level detection;
- Patents held.
Anhui Quantum Ctek Co. Ltd.

QKD Station Controller

QKD Terminal

QWDM

GHz Quantum Gateway
CV-QKD products

Terminal device (commercial product) of CVQKD in Shanghai Jiaotong University

The prototype of low speed CVQKD system

- System Frequency: 2 MHz
- Security distance: 150 km
- Secure key rate: 10 bps
- completion time: 2014

The prototype of low speed CVQKD system

- System Frequency: 25 MHz
- Security distance: 50 km
- Secure key rate: 52 kbps
- Transmitter: 4U case
- Receiver: 4U case
- completion time: 2014
Some QKD applications in China

- Chinese leaders experience QKD communications
- QKD in financial market
- Fast decision making with the help of QKD
Measurement-device-independent QKD

The first MDI-QKD experiment around the world.

- Developed up-conversion single-photon detector with high efficiency and low noise;
- The technology of interfering two independent lasers;
- immune to all hacking strategies on detection

MDI QKD

MDI-QKD system over 200km was demonstrated by Yan-Lin Tang et al. from USTC.

- Superconducting single-photon detectors with detection efficiency over 40%;
- 75MHz fully automatic and highly stable system with timing, spectrum and polarization calibration.

Laboratorial experiment

Field test in Hefei, China

The phase reference frame calibration part is intrinsically rejected in this phase coding MDI-QKD system:
- Faraday-Michelson interferometers for state preparation
- Reduces the consumption of resources, potential security flaws in practical system

8.3098 bps @1MHz

A positive secure key rate can be distilled in the experiment, with a bit error rate of 28% in the lab.

Promising for applications and networks under some extreme conditions.


Shuang Wang et al., “Experimental demonstration of quantum key distribution without monitoring of the signal disturbance” Nat Photonics. accepted 2015.9.14
Continuous-variable quantum key distribution with 1 Mbps secure key rate

Duan et al., Optics Express 23, 17511 (2015).
Open questions

- “How to measure the complexity of quantum attack” – NIST team ETSI/QSC 2013
- How to construct a secure computing science and what is the corner stone of the QSC?
- Which way is the best way to use QKD?
- When and how PQC meets QKD