Standardization of Quantum Cryptography in China

Zhengfu Han
University of Science and Technology of China
Anhui Asky Quantum Technology Co., Ltd
November 7, 2018
CONTENTS

1. Background on Quantum Cryptography
2. Standardization of Quantum Cryptography
3. Introduction on Quantum Cryptography Standards
4. Roadmap of Quantum Cryptography Standards
Necessity

Quantum cryptography can be applied to the information security fields of government, military, finance, electricity, taxation, and customs.
Background on Quantum Cryptography

Roadmap of quantum cryptography

- Standardization
  - Security
  - Application
- Cost
- Application
- Network
- Performance
  - Tel/Fax
  - Multimedia
  - Authentication
- Quantum route/switch
- Integration with existing networks
  - Secure key rate
  - Maximum safe distance
  - Stability, Usability
Cryptography Standardization Technical Committee:

Responsibilities for the standardization of cryptographic technology, product, system management, etc.
Quantum cryptography standard workgroup had been set up by the Cryptography Standardization Technical Committee in November 2012.

The workgroup lead by Anhui Asky Quantum Technology Co., Ltd.
Tasks of Quantum cryptography standard workgroup

- To formulate the QKD standards system and make a developing plan
- To draw the relation companies, scientific institutions, and the experts of university into the working group
- To investigate the user, sales, products designer, and also the security requirements to QKD
- To draft and revise the standards
- To Training engineer and consulting
- Popularization and application
- To promote international cooperation and participate in the International Organization for QKD Standards
Many companies became members of the QKD workgroup.

Many interest committees, such as communication companies, energy industries, finance and government agents, participated in the standardization of quantum secure communication.
Standardization of Quantum Cryptography

Seminars of Quantum Cryptography Standards

- 2015 Langfang
- 2016 Beijing
- 2017 Beijing
- 2018 Suzhou
<table>
<thead>
<tr>
<th>Time</th>
<th>Project Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>Technology Specification of Network Cryptographic Server Based on QKD Technology</td>
</tr>
<tr>
<td>2016</td>
<td>Technology Specification of Decoy BB84 QKD Protocol</td>
</tr>
<tr>
<td>2017</td>
<td>Report on Encrypted Communication Technology Framework Based on QKD Technology</td>
</tr>
<tr>
<td>2018</td>
<td>Research on Quantum Random Number</td>
</tr>
<tr>
<td>2018</td>
<td>Decoy BB84 QKD Test Specification</td>
</tr>
<tr>
<td>2018</td>
<td>Research on Relay Security of QKD Network</td>
</tr>
<tr>
<td>2018</td>
<td>Quantum Key Application Interface Specification</td>
</tr>
<tr>
<td>2018</td>
<td>Coherent State Continuous Variable QKD Technology Specification</td>
</tr>
</tbody>
</table>
## Working Contents

### Technology of quantum key application

- **Technology requirements of key application**
  - Key application interface
  - …..

- **Device requirements of key application**
  - Quantum VPN
  - Quantum encrypter
  - …..

- **Requirements of system and application**
  - Business requirements and application scenario
  - Network architecture
  - Network operation management

### Technology of quantum key management and device management

- **Technology requirements of key management**
  - Key management
  - Key relay
  - Key service interface
  - …..

- **Technology requirements of device management**
  - Device management interface
  - Device communication protocol
  - …..
Standardization of Quantum Cryptography

Working Contents

Technology of quantum key distribution

- Requirements of QKD protocol
  - Decoy BB84 protocol
  - Continuous variable protocol
  - …..

- Technical requirements of quantum channel
  - Quantum repeater
  - Routing and exchange
  - Channel multiplexing

- Technical requirements of quantum security
  - Security of QKD
  - Security of component and device
  - Security of interface

Test technology of quantum cryptography

- Protocol test
  - …..

- Performance test
  - …..

- Security test
  - …..
1. Background on Quantum Cryptography
2. Standardization of Quantum Cryptography
3. Introduction on Quantum Cryptography Standards
4. Roadmap of Quantum Cryptography Standards
Decoy BB84 Quantum Key Distribution Technology Specification

- Described the procedure of the decoy BB84 quantum QKD protocol. Specified the security indicators of each stage, and the technical requirements of the product functions, performance and management.

Decoy BB84 Quantum Key Distribution Test Specification

- Specified the test purpose, environment configuration, process and judgment of the decoy BB84 QKD protocol. Described the testing requirements and methods of the products function, performance, hardware, software and safety management.
## Decoy BB84 Quantum Key Distribution Technology Specification

<table>
<thead>
<tr>
<th>Sections</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 Scope</td>
<td>Application scope and specification boundaries</td>
</tr>
<tr>
<td>02 Normative references</td>
<td>Documents referenced in this specification</td>
</tr>
<tr>
<td>03 Terms and definitions</td>
<td>Terms, definitions, symbols and abbreviated terms in this specification</td>
</tr>
<tr>
<td>04 Symbols and abbreviated terms</td>
<td></td>
</tr>
<tr>
<td>05 Overview</td>
<td>QKD applications in communication system, architectures of QKD system, deployment requirements of QKD products, authentication requirements of QKD protocol</td>
</tr>
<tr>
<td>06 Quantum key distribution protocol</td>
<td>Technology requirements of QKD protocol, including quantum state preparation, quantum state transmission, quantum state measurement, basis sifting, error correction, privacy amplification and authentication</td>
</tr>
<tr>
<td>07 Product requirements</td>
<td>Including products function, performance, hardware, software and safety management</td>
</tr>
</tbody>
</table>
### Decoy BB84 Quantum Key Distribution Test Specification

<table>
<thead>
<tr>
<th>Sections</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 Scope</td>
<td>Application scope and specification boundaries</td>
</tr>
<tr>
<td>02 Normative references</td>
<td>Documents referenced in this specification</td>
</tr>
<tr>
<td>03 Terms and definitions</td>
<td>Terms, definitions, symbols and abbreviated terms in this specification</td>
</tr>
<tr>
<td>04 Symbols and abbreviated terms</td>
<td></td>
</tr>
<tr>
<td>05 Overview</td>
<td>Contents of this Specification, Relationship of Communication and QKD System, Authentication of QKD, Requirement of Assemblage</td>
</tr>
<tr>
<td>06 Test contents</td>
<td>Test contents and methods about the QKD protocol and products</td>
</tr>
<tr>
<td>07 Test methods</td>
<td></td>
</tr>
<tr>
<td>08 Conformity assessment</td>
<td>Conformity assessment of the QKD products</td>
</tr>
</tbody>
</table>
Introduction on Quantum Cryptography Standards

Technical Contents

• Basis error
• Quantum state error
• Light intensity accuracy
• Phase randomness

Quantum state preparation

• Correct of coding process
• Information leakage prevention

Quantum state transmission

• Correct of decoding process
• Detection

Quantum state measurement

• Protocol conformance in the basis sifting process

Basis sifting

• Protocol conformance in the error correction process

Error correction

• Protocol conformance in the privacy amplification process

Privacy amplification

• Protocol conformance in the authentication process

Authentication
Introduction on Quantum Cryptography Standards

Technical Contents

- Device initialization
- Function of QKD
- Key management

- Randomness of Quantum Key
- Quantum key generation rate
- Maximum distance of QKD

- Interface
- Random number generator
- Environmental adaptability
- Reliability

- Software security
- Application program interface
- Management tools

- Key management
- Data management
- Remote control management
- Device management
A first versions of the “Decoy BB84 Quantum Key Distribution Test Specification” has been formed, and will be reviewed.

A draft of the “Decoy BB84 Quantum Key Distribution Technology Specification” is calling for public comments.
Goals

◆ Completion of quantum cryptographic standardization system until 2025

➢ Establish technical standards to construct quantum cryptographic networks which integrate with traditional optical networks.

➢ Establish application standards to realize the application of quantum cryptography in traditional communications.

➢ Establish security standards for quantum secure communication systems.
Roadmap of Quantum Cryptography Standards

Quantum Cryptography Standard System Architecture

Including seven parts

01 Basic

- Application
  - Cryptography Industry
  - Communication Industry
  - Financial Industry
  - Electric Industry
  - …

- Business
  - Application Service
  - System Architecture
  - Networking Technology
  - Operation Management

02 Key Application Technology

03 Key Management Technology

- Key Agreement Management
- Key Relay Management
- Key Management
- Device Management

04 Key Agreement Technology

- Quantum key Distribution Protocol
- Quantum key Distribution Device
- Quantum Channel Multiplexing Technology
- Quantum Component

05 Quantum Cryptography Correlative technology

- Quantum Random Number
- Quantum Certification
- Quantum Public Key
- Quantum Relay
- Quantum Information Encryption
- Quantum Error Correction
- Quantum Computing

06 Security

- Evaluation System
- Safety Management
- Protocol Security
- System/Device Security
- Component Security
- Algorithm Security

07 Detection and Evaluation

Including seven parts
THANKS

E-mail: zfhan@ustc.edu.cn      Tel: +86 0551-63607342

Anhui Asky Quantum Technology Co., Ltd