International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/2020)

XSTR-SEC-QKD

Security considerations for quantum key distribution network

ITU-T

Summary

Quantum safe cryptography is becoming increasingly important in light of the challenge it faces from quantum computers.

Quantum key distribution (QKD) is a technology using quantum physics to securely exchange symmetric encryption keys. This technology solves the problem of key distribution by allowing the exchange of cryptographic keys between two remote parties with information-theoretic security, guaranteed by the fundamental laws of physics. These keys can then be used securely with conventional cryptographic algorithms.

Post-quantum cryptography (PQC) refers to cryptographic algorithms which are resilient to attacks by quantum computers. Some post-quantum cryptographies, such as lattice-, code- or hash-based cryptosystems, are currently believed to be quantum-safe until proven otherwise.

These two technologies, i.e., QKD and PQC are two pillars complementary to each other for quantum-safe cryptography. QKD can be used as a key establishment alternative and QKD deployment is used to secure operators' backbone communications. PQC is a collection of cryptographic algorithms considered to be secure against quantum computer for end-point security.

This Technical Report only studies the perspective of QKD. Although QKD technologies have been developed for several decades, there is a need to develop a QKD framework to satisfy requirements from the telecom network's perspective.

Keywords

Quantum, quantum key distribution, security.

NOTE – This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Table of Contents

Introduction

Due to advances in quantum information technologies in recent years, quantum computation and secure quantum communications will have profound impacts on information and communication technology (ICT) networks.

Quantum computing can effectively solve some mathematical problems which are difficult for classical computers, e.g., large integer factorization problem, discrete logarithms problem, and database search. At present, several famous quantum algorithms, e.g., Shor's and Grover's algorithms, are able to threaten the currently widely used cryptosystem. The preliminary impact is evaluated by several organizations, e.g., NIST [b-NIST Tech. Rep. 2016] and ETSI [b-ETSI EG 203 310]. Table 1 partially summarizes NIST's evaluation.

Table 1 – Impact of quantum computing on common cryptographic algorithms [b-NIST Tech. Rep. 2016]

Cryptographic algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	–	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

The threats posed by quantum computing have a wide range of impacts since public key algorithms such as Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC) are widely used in various security protocols and applications. How to design quantum-safe cryptography that can resist quantum computing attacks is a problem that must be considered for ICT systems to ensure security in the "quantum era".

In general, there are three possible means to combat quantum computing attacks:

1) **Enhancement of current crypto system**: Doubling the current key size can resist Grover's algorithm which provides a quadratic speed-up for quantum search algorithms in comparison to search algorithms on classical computers. However, this is only suitable for symmetric key systems.

2) **Design of new public key system**: Utilizing new mathematical problems which have not been cracked by current quantum algorithms, e.g., lattice-based and code-based cryptography algorithms, which are more often called post-quantum cryptography (PQC). However, even if those new mathematical problems might be proven as robust against known quantum algorithms, they will not be proven secure against quantum algorithms that might be created in the future.

3) **Use of QKD to replace public key based key exchange mechanism**: The security of quantum key distribution (QKD) is based on quantum physics principles, which can effectively avoid the threats caused by the increase of computational power or algorithmic "backdoors" faced by traditional public key algorithms. QKD is already proven as robust against quantum algorithms that might be created in the future.

For existing ICT systems, PQC based on traditional mathematical paradigm can provide a smoother migration to quantum-safe mode, although it cannot guarantee long term security (possible to be cracked by new quantum algorithms or crypto analysis). Thus, security evaluation and standardization are important to PQC, which is ongoing in NIST [b-NIST Tech. Rep. 2016], ETSI TC Cyber [b-ETSI EG 203 310], ISO/IEC JTC 1 SC 27 WG 2 [b-ISO SC 27 WG2 SD8] and ITU-T SG17 Q6 [b-ITU-T X.5Gsec-q]. Recent update suggests that a draft standard from NIST is expected to come into force in 2022-2023 [b- Chen2018].

For QKD, remarkable progresses have been achieved from research to practice globally, notably the "Micius" quantum science satellite, the 2000 km Beijing-to-Shanghai QKD backbone, and practical applications of many metropolitan QKD networks. However, QKD, as a new paradigm to provide security service via physical quantum communication systems, also faces a lot of challenges, e.g., cost, performance, and channel availability, which require multi-disciplinary collaborations and joint standardization efforts to bring QKD into practical security services in real world.

Technical Report ITU-T TR.SEC-QKD

Security considerations for quantum key distribution network

1 Scope

This Technical Report provides security considerations for quantum key distribution (QKD) network. It describes the following:

– Introduction to the QKD network (QKDN);

– Security considerations in communications between the QKD systems and (cryptographic) applications;

– Security considerations in communications between QKD systems and management (and monitoring) systems; and

– Standardization issues and suggestions for future works.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

3.1.1 classical channel [b-ETSI GR QKD 007]: Communication channel that is used by two communicating parties for exchanging data encoded in a form that may be non-destructively read and fully reproduced.

3.1.2 quantum channel [b-ETSI GR QKD 007]: Communication channel for transmitting quantum signals.

3.1.3 quantum key distribution (QKD) [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.1.4 key manager (KM) [b-ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node (see 3.1.11) to perform key management in the key management layer.

3.1.5 key manager link [b-ITU-T Y.3800]: A communication link connecting key managers (KMs) to perform key management.

3.1.6 quantum key distribution link [b-ITU-T Y.3800]: A communication link between two quantum key distribution (QKD) modules to operate the QKD.

NOTE – A QKD link consists of a quantum channel for the transmission of quantum signals, and a classical channel used to exchange information for synchronization and key distillation.

3.1.7 quantum key distribution module [b-ITU-T Y.3800]: A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

NOTE 1 – In this technical report, "QKD protocol" means "list of steps for establishing symmetric cryptographic keys with information-theoretical security based on quantum information theory."

NOTE 2 – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

3.1.8 quantum key distribution network (QKDN) [b-ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

NOTE – A QKDN allows sharing keys between QKD nodes by key relay when they are not directly connected by a QKD link.

3.1.9 quantum key distribution network controller [b-ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

3.1.10 quantum key distribution network manager [b-ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

3.1.11 quantum key distribution node [b-ITU-T Y.3800]: A node that contains one or more quantum key distribution (QKD) modules protected against intrusion and attacks by unauthorized parties.

NOTE – A QKD node can contain a key manager (KM).

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
API	Application Programming Interface
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMS	Element Management System
ICT	Information and Communication Technology
IP	Internet Protocol
IPSEC	Internet Protocol Security
IT-secure	Information-Theoretically secure
KM	Key Manager
LTE	Long Term Evolution
MDI-QKD	Measurement Device Independent QKD
NMS	Network Management System
OTP	One-Time Pad
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution

QKDN	QKD Network
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
WDM	Wavelength Division Multiplexing

5 Introduction to the QKDN

Quantum key distribution (QKD) technology permits the exchange of secret keys between two parties directly connected through a point-to-point QKD link.

The concept of QKD network (QKDN) needs to be introduced by extending the point-to-point topology of QKD link to a multi-hop topology in order to share information-theoretically secure (IT-secure) keys between any user applications even when they are not directly connected via a QKD link. There are mainly three possible means to build a QKDN:

– The optical switch scheme can only be used in small scale network and cannot extend QKD distance limited by quantum channel attenuation.

– The trusted relay scheme, stores keys and relays them to the next hops through secure encryption. The trusted relay using one-time pad (OTP) is the current practical solution widely adopted in QKDNs.

– The quantum relay scheme is the ideal solution to relay qubits to long distance but the required quantum memory and quantum repeater technology are currently not available.

The two adjacent QKD nodes are connected via a QKD link and a key management (KM) link:

– A QKD link consists of a quantum channel and a classical channel. The quantum channel is a physical optical path that is only used to transmit qubits. The classical channel, which is used to exchange information such as key synchronization and key distillation, can be a conventional Internet protocol (IP) channel that is not necessarily optical.

  Note that it is possible for the quantum and classical channels to share a common fibre via wavelength division multiplexing (WDM).

– The KM link is also a classical channel connecting KM or key management functional modules. Key management functions include all activities performed on keys during their life cycle such as receiving them from QKD modules, storing, relaying, deleting, and supplying them to service applications where they are used.

  Note that it is possible for the KM link and classical channel of QKD link to share a common physical link.

Any two end-to-end QKD nodes can reach each other via multi-hop QKD route through relay nodes. This QKD route can distribute the end-to-end key via OTP encryption based on the keys produced on each QKD link, which ensures key distribution across the network built only on information-theoretically secure protocols.

The control functions of the QKDN are often provided by a QKDN controller in some configurations. Those functions include authentication and authorization control, routing control of key relay, charging policy control, etc.

A QKDN manager assumes the role of monitoring and managing the QKD network to take care of fault, configuration, accounting, performance and security as a whole. Those functions are performed by gathering information about status and performances of QKD nodes, QKD links, and KM links. Consequently, communication between the QKDN controller, if there is any, and the QKDN manager as well as between QKD nodes and the QKDN manager is necessary in the QKD network.

The shared keys generated in the QKD network are delivered to service applications via flexible application programming interface (API), and the applications can perform secure communication based on QKD.

NOTE – A broader description of QKDNs is presented in clause 8 and Appendix I of [b-ITU Y.3800]

6 Security considerations for QKDN

The main purpose of QKDN is to provide keys to any users or applications which require a high-level of security.

The keys generated by QKD protocol operate by two entities, for example, sender (Alice) and receiver (Bob), can be proven as information-theoretically secure based on the quantum information theory. Their security is proved under the assumption that Alice and Bob are in physically secure locations and are also directly connected by an optical line or free space that is a point-to-point link.

Even though such a point-to-point QKD link is secure, QKDNs are composed of many nodes and links and have to securely provide keys to applications connected to any of the nodes. Consequently, this Technical Report takes into consideration ways to achieve security in the following areas:

- Key relaying functions in QKDNs;
- Security considerations in communications between QKD systems and (cryptographic) applications; and
- Security considerations in communications between QKD systems and management (and monitoring) systems.

QKDNs usually have four elements of hierarchy consisting of: cryptographic applications, QKDN controller, key management element or KM (key providing service), and key providing element (QKD modules). All the elements should be connected to the QKDN manager such as element management system (EMS), network management system (NMS) and so on. All these entities can be operated in different network topologies. All connections between entities in the same layer or between entities in the different layers should be secured by adequate cryptographic methods.

All security considerations for QKDN are addressed in this Technical Report, except for the security in the service application element which is outside the scope of this Technical Report as it is well-defined and well-studied in conventional standards.

The details of QKDN security considerations are described in terms of three topics as stated above.

1) Key relaying functions in QKDNs

    A. A QKD link itself is secure by the quantum nature but the security of areas between QKD links, that is, intermediate nodes, is not guaranteed because keys exchanged through QKD are digitalized there.

    B. Key relaying requires other functionalities beyond QKD protocols in order to securely transmit keys in a QKD network by using keys generated by each QKD link.

    C. To maintain the information-theoretical security level, special encryption methods, are necessary.

    D. Moreover, the authentication for any sender and receiver for a key and the integrity for the key itself are necessary.

    E. Key management element and key providing element should work together to support the above functionalities. In some cases, key management element should be able to control heterogeneous key providing elements based on QKD systems made by different vendors according to different protocols and architectures at the same time.

2) Security considerations in communications between QKD systems and (cryptographic) applications

A. There are various protocols to provide keys to cryptographic applications, for example, [b-ETSI GS QKD 004] and [b-ETSI GS QKD 014].

B. To secure such protocols or APIs, the reliance on conventional secure communication methods such as TLS/SSL, HTTPS, SNMP and IPSec, among others, are vital.

C. Vendors generally use their own special APIs or various protocols for providing keys. Therefore, QKD key management layer sometimes need to deploy various interfaces and security functions at the same time.

3) Security considerations in communications between QKD systems and management (and monitoring) systems

A. Conventional management (and monitoring) methods are also available for QKDNs.

B. All elements should be securely connected to management (and monitoring) systems, only if they are operated in dedicated physical units.

C. Management (and monitoring) systems (or servers) always gather all the information about performance and status from every single unit and should also recognize any failure or any levels of events immediately.

Note that for all the above, secure communication methods are also required to be properly implemented in the whole lifecycle of keys, including generate, store, use, revoke and renew.

7 Standardization issues and suggestions for future work on QKDN

QKDN technology is continuously evolving. The challenges for QKDN standardization exist from near term issues (e.g., how to ensure security and interoperability of trusted relay based QKD network) to medium- and long-term issues (e.g., how to reduce costs via the integration of quantum and classical telecom networks, how to extend the applications of QKD, as well as how to scale up the network via quantum relay).

There are ongoing QKD related standardization activities in ETSI ISG QKD, ISO/IEC JTC1 SC27 WG3, ITU SG13 and SG17. Existing work mainly focuses on QKD link-level issues, including QKD optical components, modules, internal and application interfaces, security evaluation and certification, etc.

Wide-area network coverage and vast applications are key to drive the development of the quantum cryptography industry. The QKD network level issues, which require joint efforts from multiple disciplines including quantum physics, telecom network and information security, etc., are also important and require further standardization efforts, as summarized below.

1) Issue 1: How to ensure QKDN interoperability?

Interoperability is an important issue for wide-area QKD network in order to accommodate multi-vendor devices. However, there is still no standard to resolve this issue.

There are two possible solutions to achieve multi-vendor interoperability:

– **Key management level interoperability**: There is the need to standardize the interface between KM and QKD devices to enable the two hops of QKD links to use different vendor devices.

– **QKD link level interoperability**: There is the need to standardize the interfaces between two QKD nodes, i.e., a QKD link and a KM link, in order to enable the interoperability of QKD devices from different vendors.

The key management level interoperability is the near-term solutions, and should be standardized first.

Considering the fact that QKD protocol is still actively evolving, there may not be any urgency to standardize QKD link level interoperability as the current protocol may become outdated after the standardization of link level interfaces.

2) Issue 2: How to ensure security of trusted-relay-based QKDN?

The goal of QKDN is to provide information security services for users, in terms of secret key materials or encryptions. In a QKDN based on trusted relay, security is guaranteed by the point-to-point QKD security and classical security, such as key relays, communications between QKD and applications, and communications between QKD and management (and monitoring) systems.

Currently, QKD security study is being pursued in ETSI and ISO [b-ETSI White paper no. 27] and [b-ISO/IEC QKD work items]. However, the study of possible attacks on QKD as a starting point for the security framework for QKDN is still not available. Threat assessment of attacks on the implementations of QKDN is not been studied for the time being in any standard works.

Moreover, security requirements, techniques, mechanisms and protocols of classical security modules have been thoroughly studied [b-ITU-ICT Security Manual 2015]. However, a comprehensive study on the identifications of these classical security modules and successions of the related standards in QKDN has not been considered in any standard groups. Ultimately, it is also suggested to include PQC security requirements if PQC is considered to be merged with QKDN.

3) Issue 3: How to reduce QKD deployment cost?

Current QKD implementations usually require expensive fibre, racks, room resources and separate hardware devices. How to reduce QKD costs is important to its commercial development. The possible means include co-fibre transmission of QKD channels and existing optical transmission networks, integration of QKD modules into telecom network devices, etc.

4) Issue 4: How to extend QKD applications to more valuable scenarios?

The current QKD applications are largely limited by bulky hardware device and strict quantum channel requirements, and limited functions of QKD protocol, etc. To flourish the QKD industry, there is the need to further identify and study new application scenarios and use cases of QKD, e.g., satellite-based wide-area QKD, miniaturized and free space QKD, integration of QKD and classical cryptography including PQC.

5) Issue 5: How to scale up QKDN via quantum relay?

Although QKDN can be constructed via trusted relay, it also introduces potential security threats since keys stored in the KM memories as classical bits are no longer guaranteed by quantum physics. The merger with quantum relay and quantum repeater technologies for realizing scalable QKD network is the ultimate secure quantum communication solution. Solutions and technical requirements for quantum relay and quantum repeater technologies need to be studied in order to prepare for upcoming new technologies to extend the reach of QKDN in a real quantum manner.

In light of the global security threats as a result of quantum computing, it is suggested that ITU-T needs to pay attention and carry out systematic research on how to transfer the existing telecom infrastructure to quantum-safe mode.

As far as it concerns QKD as a new technology based on quantum communication network to provide security services, it needs to seriously consider how to coordinate and carry out standardization works efficiently and cooperatively.

For QKDN security, it is suggested to include a detailed study of metric and a benchmark on different attacks on the implementations of QKD. It is also suggested to include classical security analysis and PQC integration in the QKDN framework.

For the medium and long-term QKDN issues, such as low-cost solutions, new applications, scalability with quantum relay, it is recommended to initiate standardization studies to explore how to promote related targets efficiently.

According to the analysis in this Technical Report, there are gaps to be studied in ITU-T SG17 which should be standardized in new recommendations.

Annex A

QKD deployment examples around the world

A.1 Quantum key distribution network deployment in China

For the past decade, China has made remarkable progress in real world quantum key distribution (QKD) network demonstrations and deployments, including both metropolitan and backbone quantum network. In 2007, the first decoy-state QKD over 100 km fibre was achieved, which broke the previous limits of security distance [b-Peng2007]. In 2009, telephone voice signal encryption with quantum keys over an all-pass and inter-city quantum communication network was demonstrated [b-Chen2010]. QKD networks with wavelength division multiplexing of quantum and classical signal were tested successfully in different cities [b-Wang2010] and [b-Mao2018]. From 2011 to 2012, a long-term reliability test of more than 5 000 hours was conducted in the Hefei-Chaohu-Wuhu wide area QKD network over an intercity scale, which included a typical full-mesh core network in Hefei to offer all-to-all interconnections, and quantum access network with point-to-multipoint configuration in Wuhu [b-Wang2014]. The first measurement-device-independent QKD (MDI-QKD) was experimentally undertaken in 2013, which removes all security loophole issues on imperfect detection systems. Later on, MDI QKD network with three user nodes and one untrusted relay node was demonstrated in a real network environment (Figure1(c)) [b-Tang2016].With these achievements of QKD networks as technologies bases, in 2013 China started to build the world's longest quantum secure communication backbone network from Beijing to Shanghai with a fibre distance of over 2 000 km (Figure1(a)) [b-Zhang 2018] and [b-Zhang 2019]. Main cities between Beijing and Shanghai are connected by 32 trusted nodes in the backbone network to realize long distance QKD based on trusted relay. Four metropolitan QKD networks with different topologies, namely Beijing, Jinan, Hefei and Shanghai are connected with the backbone network. The topology of Jinan metropolitan QKD network is shown in Figure1(b). The backbone was successfully built in 2018, which provides practical applications in real world and also serves as a platform for quantum communication research. Currently real-world applications are under testing with banks, securities, and insurance users.

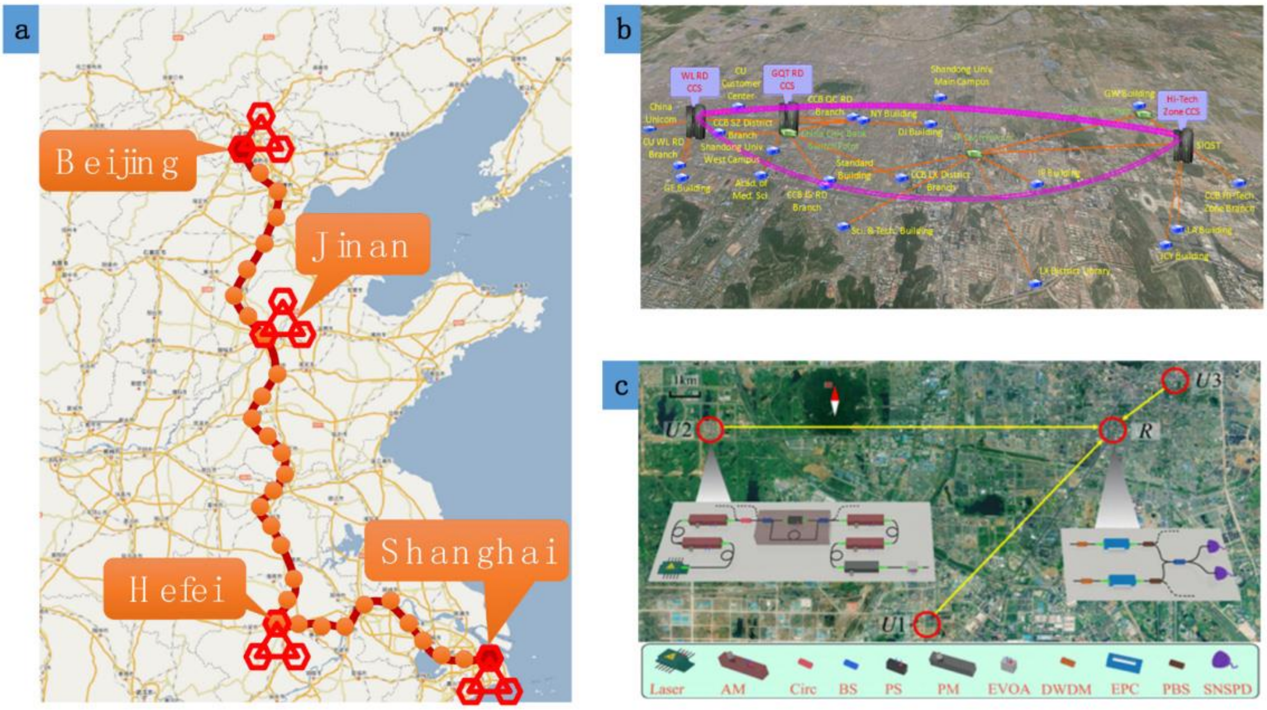

Figure A.1 – Reprint from Figure 3 of [b-Zhang2018] (a) An outline of Beijing-Shanghai 2 000 km backbone QKD network. (b) The topology of Jinan metropolitan QKD network. (c) MDI-QKD network with three user nodes and one untrusted relay node [b-Tang2016]

Besides the QKD network in fibre optics, China is also pioneering in satellite based QKD network. The world's first quantum science satellite, known as Micius, was launched in Jiuquan, China in August 2016. Micius is a LEO satellite orbiting at an altitude of about 500 km, which demonstrated decoy-state QKD with polarization encoding from the satellite to the ground for over 1 200 km with 1 kbit/s secret rate [b-Liao2017]. Later on, in 2017 Micius quantum satellite was used as a trusted relay to distribute keys between multiple locations in China and Europe to realize the first intercontinental quantum communication [b-Liao2018]. Real time video conference call encryption with quantum keys was also undertaken between Beijing and Vienna. Such work opens the door for future global QKD network with satellites.

A.2 QKD network deployment in Japan

In 2010, fast QKD systems operated at the GHz-clock were developed and used for successfully demonstrating one-time pad (OTP) encrypted video conference in Tokyo QKD network over a metropolitan area, interconnecting various different types of QKD systems [b-Sasaki2011]. Since then, long-term reliability tests of QKD network is being extensively investigated in Tokyo QKD Network [b-Dynes2012], [b-Yoshino2013], [b-Shimizu2014], [b-Dixon2015] and [b-Dixon2017].

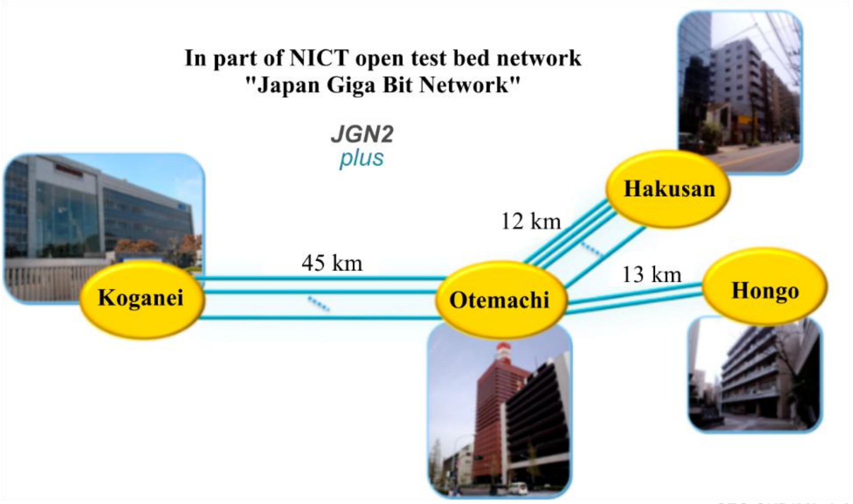

Figure A.2 – Tokyo QKD network

As various QKD networks have been operating in realistic field environments, studies on integrating a QKD network into an optical communications infrastructure has started addressing what kinds of security threats are most likely, how security can be enhanced by introducing a QKD network, and what would be an appropriate architecture for the integration [b-Kitayama2011], [b-Sasaki2015]. Research and development on cryptographic applications based on a QKD network is actively underway. Integration methods of a QKD network into an Internet infrastructure have been developed in the form of QKD-secured Layer-2 and Internet protocol (Layer-3) switches [b-Fujiwara2015]. QKD networks enable a new application such as quantum digital signature, and this has been deployed on Tokyo QKD network [b-Collins2016] and [b-Collins2017].

Although QKD enables the information theoretic security (confidentiality) of data transmission, QKD itself cannot protect confidentiality of data storage. On the other hand, digital data stored in data centres may easily be targeted by malicious attacks or even be threatened by non-malicious incidents like natural disasters. Sensitive data relevant to human genome and health require protection throughout their lifetime or even a longer time for several generations, which may be a century time scale. Computationally secure cryptographic schemes can provide no clue for its security over such a long term. QKD network technologies have recently been combined with secret sharing technique for distributed storage to realize information theoretic confidentiality of data storage [b-Fujiwara2016] and [b-Braun2017]. The combined system is referred to as the long-term, integrity, authenticity, and confidentiality protection system (LINCOS). LINCOS is implemented in Tokyo QKD network, and tested with sample data of standardized medical record format.

Through these research and development, QKD network architectures have also been studied, and there have been significant advances in key management methods and application program interfaces [b-Tajima2017], [b-Sasaki2017] and [b-Sasaki2018].

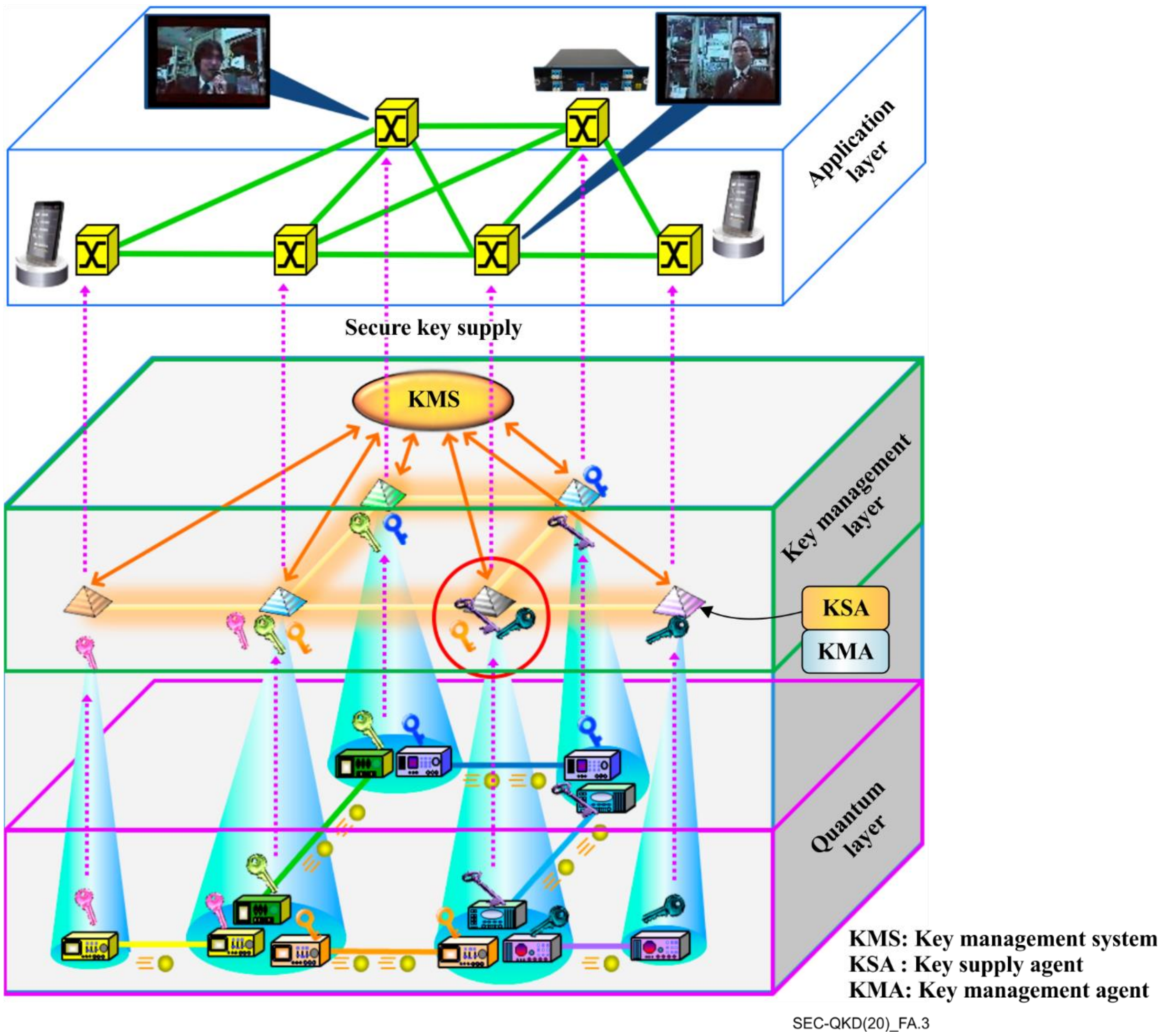

Figure A.3 – A QKDN architecture and applications

A.3 QKD network deployment in South Korea

The first commercial QKD network was deployed in South Korea in June 2016. This network applied QKD to long term evolution (LTE) backhaul between Sejong central office and Daejeon central office of SK telecom [b-SKTelecom QKD 2016].

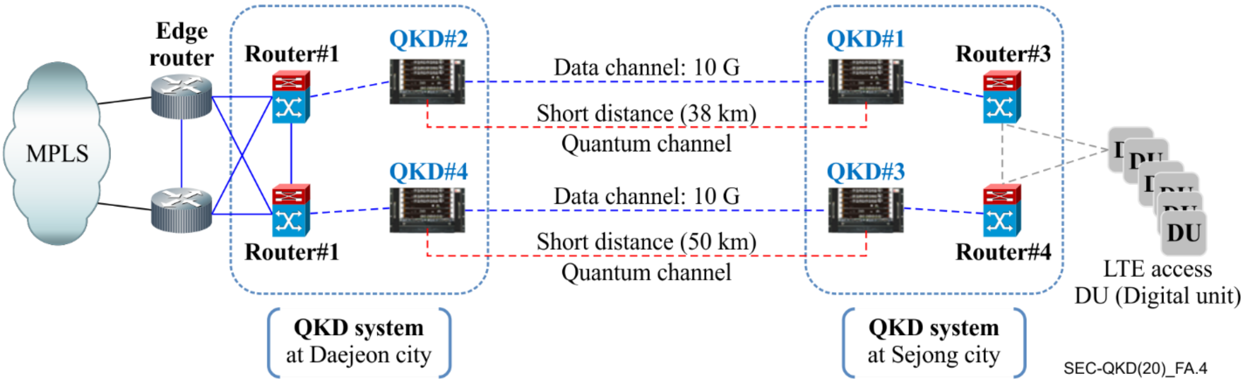

Figure A.4 – Representation of QKD network deployment in LTE backhaul in South Korea

A trusted relay node was implemented for long distance QKD network for a total of 221 km of transmission line between Sungsu central office (Seoul area) and Dunsan central office (Daejeon area) of SK telecom in 2018. It will be extended to Taepyung central office (Daegu area) and this will make the end to end distance 380 km [b-SKTelecom QKD 2019].

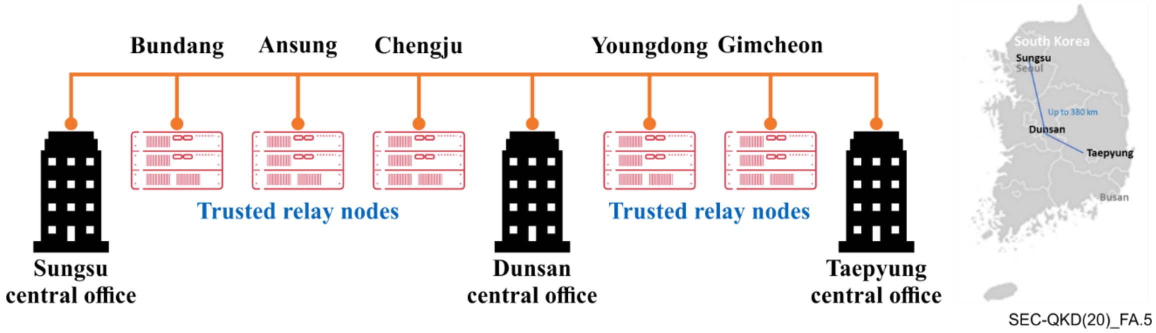

Figure A.5 – Representation of long distance QKD network deployment in LTE and 5G backhaul in South Korea

A.4 QKD network deployment in Switzerland

A QKD network testbed was deployed in Geneva, Switzerland from March 2009 to January 2011. This testbed, called SwissQuantum network, was composed of three QKD nodes within the Geneva area. Quantum transceivers, quantum key managers and applications were installed in each of these nodes. During SwissQuantum testbed, the consumption of keys provided by a QKD network was demonstrated for three different applications: commercial high-speed Layer 2 encryptors (10 Gbit/s Ethernet); research encryption and authentication platforms working at Layer 2 and IPSec encryptors. The quantum key managers were able to distribute keys between the three nodes and to generate hybrid keys, by combining key exchanged through QKD with keys exchanged through public key interfaces. The quantum transceivers were able to exchange more than 300'000 AES-256 keys over more than 600 days.

More technical details on SwissQuantum testbed and its performance can be found in [b-Stucki].

Annex B

Gap analysis

NOTE – This annex was developed with information available as of June 2019.

B.1 ETSI standardization activities and the proposed work at ITU-T SG17 on QKD

Within ETSI, an industry specification group was established in 2008 to work on the definition of industry specification documents on quantum key distribution (QKD).

NOTE – In the present gap analysis only the published documents are considered. All documents in another status (as early draft stage, stable draft stage, final draft stage, withdrawn, or stopped) are not included in this gap analysis as they are moving targets which means nobody would know what would be the final contents when they are approved and published.

So far, the following table of documents are published, approved pending publication or in the drafting stage:

Identification	Status
DGS/QKD-002_UserReqs ETSI GS QKD 002 V1.1.1	Published
DGS/QKD-003_CompInternInterf ETSI GR QKD 003 V2.1.1	Published
DGS/QKD-004_ApplIntf ETSI GS QKD 004 V1.1.1	Published
RGS/QKD-004ed2_ApplIntf	Drafting stage
DGS/QKD-005_SecProofs ETSI GS QKD 005 V1.1.1	Published
DGR/QKD-0007_Ontology ETSI GR QKD 007 V1.1.1	Published
DGS/QKD-008_SecSpec ETSI GS QKD 008 V1.1.1	Published
DGS/QKD-010_ISTrojan	Drafting stage
DGS/QKD-011_OptCompChar ETSI GS QKD 011 V1.1.1	Published
DGS/QKD-012_DeployParam ETSI GS QKD 012 V1.1.1	Published
DGS/QKD-013_TransModChar	Drafting stage
DGS/QKD-014KeyDeliv ETSI GS QKD 014 V1.1.1	Published
DGS/QKD-015_ContIntSDN	Drafting stage

A QKD system is composed of two devices. One of them is the QKD emitter, and the other is the QKD receiver. Both devices are connected together through two communication links, i.e., the quantum channel and the classical channel. The quantum channel is a unidirectional quantum communication link. The classical channel is a bidirectional communication link that can be implemented with various communication protocols, e.g., Ethernet protocol.

Each QKD device can be decomposed in components as follows:

- **Quantum platforms**, known as quantum emitter and quantum receiver, are used to emit and measure the quantum states that travel with the quantum channel. The quantum platforms are used to exchange what is called the raw keys between the emitter and the receiver;
- **Key distillation platforms** are used to estimate the maximum information that an eavesdropper can have on the raw keys and then extract secret keys when possible from those raw keys. Both key distillation platforms communicate through the classical channel;
- **Key management platforms** are used to manage the secret keys generated by the distillation platforms. The main tasks of key management platforms are key storage, key formatting, key delivery to the application and key erasure;
- **Application interfaces** are interfaces between the QKD and applications to allow the delivery of the secret keys;
- **System management platforms** are used to coordinate the proper functioning of the different platforms within one QKD device and to provide auxiliary functions as user interface;
- **Management interface platforms** are used to connect the management system to a network management system.

The scope of each published ETSI documents is described in the following list:

- GS QKD 002 covers a description of QKD use-cases. All those use-cases consider point to point direct link connection between two QKD users. This ETSI document can impact all components.
- GR QKD 003 covers a description of the components and internal interfaces in a QKD device. This ETSI document impacts quantum emitter and quantum receiver components.
- GS QKD 004 covers a description of an application interface. This ETSI document impacts the application interface component.
- GS QKD 005 covers a description of security proofs of QKD protocols. This ETSI document can impact all components.
- GS QKD 008 covers a description of the module security specifications, e.g., the physical security of the QKD device or the security of the QKD external interfaces. This ETSI document can impact all components.
- GS QKD 011 covers a description of the characterization of the optical components in a QKD device. This ETSI document impacts quantum emitter and quantum receiver components.
- GS QKD 012 covers a description of the main communication resources involved in a QKD system and the possible architectures that can be adopted when performing a QKD deployment over an optical network infrastructure. This ETSI document can impact the quantum and classical channels and the management and application interfaces.
- GS QKD 014 covers a description of the module security specifications, e.g., the physical security of the QKD device or the security of the QKD external interfaces. This ETSI document can impact the application interface.

The study of security considerations of three specific areas of a QKD network in SG17 are as follows:

1) Key relaying functions in QKDNs;
2) Security considerations in communications between QKD systems and applications (cryptographic applications) communication entity; and
3) Security considerations in communications between QKD systems and management (and monitoring) systems.

A QKD network can be built on top of a network of point to point QKD links. This QKD network can be seen as an overlay network providing secret key delivery as a service. This overlay network is mainly composed of a key manager (KM) running in servers located in each node of this network. The scope of the work at ITU-T SG 17 on QKD is limited to the security considerations of the interactions between (1) KMs, (2) the KMs and the applications, and (3) between the network management system and the node containing one KM and several QKD devices.

B.2 ISO/IEC standardization activities and the proposed work at ITU-T SG17 on QKD

In ISO/IEC JTC1 SC27, there are two new work item proposals which were ratified in March 2019 and they were in working draft phase as of December 2019.

The proposed International Standard specifies the security requirements, test and evaluation methods for QKD. Specifically, it will define a general framework for the security evaluation of QKD under the framework of ISO/IEC 15408, by specifying the common security requirements for the optical and classical cryptographic components of QKD, and specializing the security requirements for some mature enough protocols and their implementations respectively, including decoy-state BB84 QKD, measurement-device-independent (MDI) QKD and continuous-variable (CV) QKD. Then the security evaluation and testing methods for QKD components, including the optical components and classical cryptographic components will be specified.

As QKD modules are essentially cryptographic modules, the proposed International Standard is closely related to ISO/IEC 15408 and ISO/IEC 19790 for security requirements characterization and testing methods description, and can be considered as their applications in specialization area of QKD technology.

Since ISO/IEC JTC1 SC27 will mainly focus on the security requirements and evaluation methods of QKD device itself, it means that ISO/IEC will not deal with the security requirements on the network aspects from the operators' perspective. In turn, it can be concluded that there is no gap between ISO/IEC works and ITU-T SG17 works.

Bibliography

[b-Braun2017] J. Braun, et al., *LINCOS: A Storage System Providing Long-Term Integrity, Authenticity, and Confidentiality,* ' Proc. of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIACCS), pp. 461-468, Apr. (2017).

[b-Chen2010] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, *Metropolitan all-pass and inter-city quantum communication network*, Opt. Express 18(26), 27217-27225 (2010).

[b-Chen2018] L. Chen, *NIST PQC Standardization- The first round candidates*, ETSI/IQC Quantum Safe Workshop 2018.

[b-Collins2016] R. J. Collins, et al., *Experimental transmission of quantum digital signatures over 90-km of installed optical fiber using a differential phase shift quantum key distribution system*, Opt. Lett. Vol. 41, No. 21, pp. 4883-4886, Nov. (2016).

[b-Collins2017] R. J. Collins, et al., *Experimental demonstration of quantum digital signatures over 43 dB channel loss using differential phase shift quantum key distribution,* Scientific Reports Vol. 7, pp. 3235(1)-3235(8), Jun. (2017).

[b-Dixon2015] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, *High speed prototype quantum key distribution system and long term field trial,*' Optic Express Vol. 23, No. 6, pp. 7583-7592, Mar. (2015).

[b-Dixon2017] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, W. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M, Fujiwara, M. Sasaki, and A. J. Shields, *Quantum key distribution with hacking countermeasures and long term field trial*, Scientific Reports Vol. 7, pp. 1978(1)-1978(9), Aug. (2017).

[b-Dynes2012] J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara,M. Sasaki, and A. J. Shields, *Stability of high bit rate quantum key distribution on installed fiber*,' Opt. Express Vol. 20, No. 15, pp. 16339-16347 (2012).

[b-ETSI EG 203 310] ETSI EG 203 310 (V1.1.1): *CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection*.

[b-ETSI GS QKD 004] Group Specification ETSI GS QKD 004 (2010), *Application Interface*.

[b-ETSI GS QKD 007] Group Specification ETSI GS QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary*.

[b-ETSI GS QKD 014] Group Specification ETSI GS QKD 014 (2019), *Protocol and data format of REST-based key delivery API.*

[b-ETSI White paper no. 27] ETSI White paper No. 27, *Implementation Security of Quantum Cryptography*.

[b-Fujiwara2015] M. Fujiwara, T. Domeki, S. Moriai, and M. Sasaki, *Highly Secure Network Switches with Quantum Key Distribution Systems,*' Int. J. of Network Security Vol. 17, No. 1, pp. 34-39, Jan. (2015).

[b-Fujiwara2016] M. Fujiwara, et al., *Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing,*' Scientific Reports Vol. 6, pp. 28988(1)-28988(8), July (2016).

[b-ISO/IEC QKD work items] ISO/IEC JTC1 SC27 WG3, *Security requirements, test and evaluation methods for quantum key distribution*.

[b-ISO SC 27 WG2 SD8] ISO/IEC JTC1 SC27 WG2, *Standing Document 8(SD8) on Post-Quantum Cryptography*.

[b-ITU-ICT Security Manual 2015] ITU ICT Security Manual, 2015 *Security in Telecommunications and Information Technology*.

[b-ITU-T SG17 Q6 X.5Gsec-q] ITU-T SG17 Q6, *Security guidelines for applying quantum-safe algorithms in 5G systems*.

[b-ITU-T X.pqsym] ITU-T SG17 Q11, *Post-quantum symmetric encryption algorithms*.

[b-ITU-T Y.3800] Recommendation ITU-T Y.3800, *Overview on networks supporting quantum key distribution.*

[b-Kitayama2011] K. Kitayama, et al., *Security in photonic networks: Potential threats and security enhancement*, J. Lightw. Technol., Vol. 29, No. 21, pp. 3210–3222, Nov. 2011.

[b-Liao2017] S.-K. Liao, et al., *Satellite-to-ground quantum key distribution,* Nature Vol. 549, pp. 43–47, Sep. (2017).

[b-Liao2018] S.-K. Liao, et al., *Satellite-Relayed Intercontinental Quantum Network*, Phys. Rev. Lett. Vol. 120, No. 3, pp. 030501-1-030501-4, Jan. (2018).

[b-Liu2013] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J.S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, *Experimental measurement-device-independent quantum key distribution*, Phys. Rev. Lett. 111(13), 130502 (2013).

[b-Mao2018] Y. Mao et al., *Integrating quantum key distribution with classical communications in backbone fiber network,* Opt. Express Vol. 26, No. 5, pp. 6010-6020 (2018).

[b-NIST Tech. Rep. 2016] L. Chen, S. Jordan, etc. (2016). *NIST: Report on Post-Quantum Cryptography,* NIST, Tech. Rep.

[b-Peng2007] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan,*Experimental long-distance decoy-state quantum key distribution based on polarization encoding*, Phys. Rev. Lett. 98(1), 010505 (2007).

[b-Sasaki2011] M. Sasaki, et al., *Field test of quantum key distribution in the Tokyo QKD Network*,' Opt. Express Vol. 19, pp. 10387-10409 (2011).

[b-Sasaki2015] M. Sasaki, et al., *Quantum Photonic Network: Concept, Basic Tools, and Future Issues*,' (Invited paper) IEEE J. of Select. Topics in Quantum Electronics, Vol. 21, No. 3, pp. 6400313-1-6400313-13, May (2015).

[b-Sasaki2017] M. Sasaki, *Quantum networks: where should we be heading*?, Quantum Sci. Technol. Vol. 2, No. 2, pp. 020501-1-020501-8, Apr. (2017).

[b-Sasaki2018] M. Sasaki, *Quantum Key Distribution and Its Applications*, IEEE Security & Privacy Vol. 16, No. 5, pp. 42-48, Sep/Oct. (2018).

[b-Shimizu] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, *Performance of Long-Distance Quantum Key Distribution over 90-km Optical Links Installed in a Field Environment of Tokyo Metropolitan Area*, IEEE/OSA Journal of Lightwave Technology Vol. 32, No. 1, pp. 141-151, Jan. (2014).

[b-SKTelecom QKD 2016] https://www.fiercewireless.com/wireless/sk-telecom-develops-advanced-quantum-repeater

[b-SKTelecom QKD 2019] https://www.telecomtv.com/content/telco-and-csp/sk-telecom-continues-to-expand-its-foothold-in-the-global-quantum-cryptography-market-36657/

[b-Stucki] D. Stucki, et al., New J. Phys. 13 123001 (2011), *Long term performance of the SwissQuantum quantum key distribution network in a field environment.*

[b-Tajima2017] A. Tajima, et al., *Quantum key distribution network for multiple applications*, Quantum Sci. and Tech. Vol. 2, pp. 034003(1)-034003(9), Jul. (2017).

[b-Tang2016] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, *Measurement-device independent quantum key distribution over untrustful metropolitan network*, Phys. Rev. X 6(1), 011024 (2016).

[b-Wang2010] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, *Field test of wavelength-saving quantum key distribution network*, Opt. Lett. 35(14), 2454–2456 (2010).

[b-Wang2014] S. Wang, et al., *Field and long-term demonstration of a wide area quantum key distribution network*, Opt. Express Vol. 22, No. 18, pp. 21739–21756 (2014).

[b-Yoshino2013] K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, *Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days*, Opt. Express Vol. 21, No. 25, pp. 31395-31401, Dec. (2013).

[b-Zhang2018] Q. Zhang, et al., *Large scale quantum key distribution: challenges and solutions*, (Invited paper). Opt Express Vol. 26, No. 18, pp. 24260-24273, Sep (2018).

[b-Zhang 2019] Qiang Zhang et al 2019 Quantum Sci. Technol. 4 040503, 2019.