INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG13-TD236/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13 Geneva, 13 – 24 March 2023

TD

Source: Editors

Title: Draft new Supplement ITU-T Y.Supp.QKDN-UC: "Use cases of quantum key distribution networks"

Contact:	Chang-Yui Shin Korea University Korea (Rep. of)	Tel: +82-10-6398-0139 E-mail: realmine@korea.ac.kr
Contact:	Zhangchao Ma CAS Quantum Network Co., Ltd. China	E-mail: mazhangchao@qtict.com
Contact	Xiaosong Yu, BUPT	Email: xiaosongyu@bupt.edu.cn
Contact	Junsen Lai, MIIT	Email: laijunsen@caict.ac.cn

Abstract: This document is the output of draft Supplement ITU-T Y.Supp.QKDN-UC – "Use cases of quantum key distribution networks" (Q16/13 meeting, Geneva, 13-24 March 2023).

Summary

This TD is the output for the draft Supplement ITU-T Y.Supp.QKDN-UC – "Use cases of quantum key distribution networks" based on the following input contributions and the discussion during the Q16/13 meeting, Geneva, 13 – 24 March 2023.

Base document: **TD180/WP3**

C-382	BUPT	Proposal of providing a template for QKDN use case on Draft Y.Supp.QKDN-UC "Use cases of quantum key distribution networks"	Q16/13

- This contribution purposes to provide a template for QKDN use case according to the diversity of QKDN applications on Draft Y.Supp.QKDN-UC.

C-434	ETRI, Korea University, KT Corporation	The tables for use cases selection in TR.QN-UC and Y.supp.QKDN-UC for the JCA-QKDN meeting	Q16/13

- This contribution proposes to share the tables for use cases selection in TR.QN-UC and Y.supp.QKDN-UC to the JCA-QKDN meeting for discussion with other groups' experts.

C-436	ETRI, Korea University, KT Corporation	Proposed template for use cases analysis in Y.supp.QKDN-UC	Q16/13

- This contribution proposes a template for use cases analysis in Y.supp.QKDN-UC “Use cases of quantum key distribution networks”.

Meeting results

- Based on two input contributions (C-382 and C-436), the meeting has made a new use case template and encouraged to use this template for future contributions.
- The meeting has also agreed to introduce the tables for use cases selection in the JCA-QKDN meeting.

Annex A

Draft new Supplement ITU-T Y.Supp.QKDN-UC

Use cases of quantum key distribution networks

Summary

Based on the deliverable (D2.2) of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N), this Supplement consolidates the QKDN use cases collected from the ITU-T FG QIT4N in the context of networking technologies as the mandate of ITU-T SG13.

Through a comprehensive analysis, the QKDN uses cases are classified into several classes and this Supplement highlights the competitive advantage of the use cases brought by QKDN and provides suggestions for future standardization efforts in ITU-T SG13.

Keywords

QKDN; Quantum key distribution networks; Use cases.

Table of Contents

Page

1 Scope 4
2 References 4
3 Definitions 4
3.1 Terms defined elsewhere 4
3.2 Terms defined in this Supplement 4
4 Abbreviations and acronyms 4
5 Introduction 4
6 The competitive advantage of using QKDN 5
7 Overview of QKDN use cases 6
8 Use Cases 7

Appendix I Overview of QKDN use cases 26
I.1 UCC1: QKD combined with other cryptographic primitives 27
I.1.1 QKD combined with secret sharing 27
I.1.2 QKD combined with SMC 27
I.1.3 Hybrid QKD and PQC for encrypted communications 27
I.2 UCC2: QKD integrated with various TCP/IP protocols 27
I.2.1 QKD integrated in data link layer 27
I.2.2 QKD integrated in network layer 28
I.2.3 QKD integrated in transport layer 28
I.2.4 QKD integrated in application layer 28
I.3 UCC3: QKD implemented in various network topologies 28
I.3.1 QKDN as metropolitan access network 28
I.3.2 QKDN as inter-city backbone network 28
I.3.3 QKDN as free-space satellite-ground or inter-satellite network 29
I.4 UCC4: QKD with different user device categories 29
I.4.1 Wireless user device with offline QKD-keys 29
I.4.2 Wireless user device with integrated QKD module 29
I.5 UCC5: QKD integrated in various network forms 29
I.5.1 QKD in 4G/5G networks 29
I.5.2 QKD in SDN/NFV based network 30
I.5.3 QKD in blockchain network 31
I.5.4 QKD in TSN network 32
I.5.5 QKD in SCION 32
I.6 QKD applied in different vertical sectors 32
I.6.1 QKDN for smart factory 32
I.6.2 QKDN for social safety 33
I.6.3 QKDN for medical centre 33
I.6.4 QKDN for secure mVoIP 33

Bibliography 34

Draft new Supplement ITU-T Y.Supp.QKDN-UC

Use cases of quantum key distribution networks

1 Scope

This Supplement presents use cases of quantum key distribution (QKD) networks. In particular, the scope of this Supplement includes:

- Competitive advantage brought by QKDN;
- Overview of QKDN use cases;
- Analysis of collected QKDN use cases including categorization.

2 References

TBD

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 **<Term 1>** [Reference]: <optional quoted definition>.

3.1.2 **<Term 2>** [Reference]: <optional quoted definition>.

TBD

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

TBD

5 Introduction

This Supplement identifies foreseeable, near-term use cases of QKDN technologies gathered during the life of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). It lists and presents descriptive information about each of the use cases – for those applications and services based on QKDN technologies. These use cases were submitted by individuals within organizations from around the world and FG QIT4N only considered those use cases that had reached at least a demonstratable, proof-of-concept stage.

The Supplement first introduces the potential competitive advantage brought by QKDN to various applications and services. Then, it categorizes the collected QKDN use cases into several classes and provides an overview of each use case. Finally, it summarizes key findings, provides suggestions for further standardization and industrialization and offers a repository of all collected use cases in Appendix I.

The aims of this Supplement are to:

a) assist technology-oriented decision makers in identifying future opportunities arising from recent advances in QKDN technologies,

b) support exchange information and best practices through peer learning and knowledge dissemination processes, and

c) identify possible standardization requirements in the ITU-T SG13.

6 The competitive advantage of using QKDN

Through QKD, the two parties of communication can realize secure symmetric key agreement based on the transmission and processing of quantum states. Moreover, any eavesdropping behaviour will be discovered in time due to the disturbance of the quantum state.

QKD is different from conventional key distribution based on computational complexity because its information theoretical security is based on the principles of quantum mechanics. As long as an adversary does not violate the principles of quantum physics, even if they were to have a computer with arbitrary computing power such as a quantum computer, the security of QKD will not be affected.

Depending on the combination of QKD and conventional cryptography, the application of quantum secure communication can have multiple implementations, e.g.:

- Combining QKD with an encryption scheme (such as OTP algorithm) and an authentication scheme (such as Universal-2 hash algorithm) providing information theoretic security, a quantum secure communication system with information theoretic security can be realized.
- The combination of QKD, encryption schemes and authentication schemes that are resistant to quantum computing attacks can realize a quantum secure communication system that can resist quantum computing attacks.

As a supplementary component of cryptography, QKD has rich application scenarios. For example, it can be combined with various existing information and communication protocols at different TCP/IP layers and can also serve various industrial application scenarios to meet the highest security requirements such as providing long-term security guarantees and countering quantum computing attacks.

QKDN has the following competitive advantages:

1) Quantum computing resistance: The threats posed by quantum computing have a wide range of impacts to various security protocols and applications based on conventional asymmetric and symmetric cryptography algorithms. As the security of these algorithms relies on the computing complexity to resolve certain difficult mathematical problems, quantum computing based on quantum algorithms such as Shor's or Grover's algorithm can effectively solves these mathematical problems. As studied in [b-ETSI GR QSC 006], conventional asymmetric algorithms based on RSA and ECC would be completely broken by Shor's algorithm. For symmetric algorithms, Grover's algorithm effectively halves the key size for these algorithms. Compared with conventional computation-complexity-based cryptography, QKD can be considered as one of the means to combat quantum computing threats by replacing traditional key exchange mechanisms.

2) Perfect forward security (PFS): Conventional symmetric cryptography, which is vastly applied in mobile networks (including 2G/3G/4G/5G), and Kerberos-based enterprise systems usually rely on the pre-shared root keys and exchange of random numbers to refresh the session keys. It is not easy to change the root keys. For example, the root key for a mobile phone stored in the SIM card cannot be changed during the entire lifecycle. Once the root key is revealed, all the historical data can be decrypted. Compared to conventional symmetric cryptography, QKD systems can guarantee PFS since the keys are continuously refreshed and can thus only be used once. Even if some keys are revealed, the security of the entirety of historical data cannot be breached.

NOTE – PFS can also be achieved via asymmetric cryptography, however, conventional asymmetric cryptography may encounter the threat from quantum computing attack.

3) High performance key generation: Most internet security applications including HTTPS, software update, VPN, email and blockchain, etc. are based on asymmetric cryptography, also called public key cryptography (PKC). Quantum-computing-resistant PKC, also called post-quantum cryptography (PQC), is under rapid development and standardization. Certain asymmetric

cryptography can also provide PFS, however, asymmetric cryptography which relies on specific hard mathematical problems usually require high overhead for computing power and processing delay. Compared to asymmetric cryptography, QKD, as the key exchange method based on quantum physics means, can provide high throughput and low latency key generation which can be one attractive option for applications which require high performance, e.g., certain time-sensitive services.

7 Overview of QKDN use cases

As key distribution is one of the fundamental cryptographic primitives, QKD has very rich application scenarios which can be classified according to various perspectives, as shown in Figure 7-1.

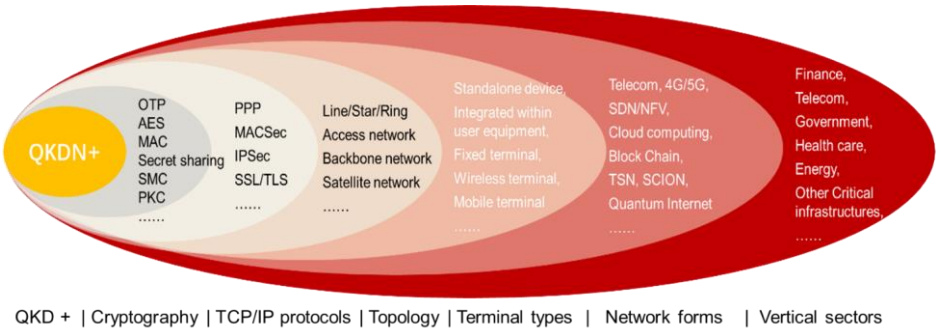

Figure 7-1 – QKDN use cases overview

(Editor's Note) The following six use classes are the result of FG-QIT4N. For selected use cases in this Supplement, it's necessary to review and categorize them again with different criteria in the context of ITU-T SG13.

In this Supplement, the collected QKDN use cases are classified into the following six use case classes (UCCs):

1) UCC1: QKD combined with other cryptographic primitives

- **Encryption**: QKD can be combined with either OTP or AES to perform symmetric encryption;
- **Message authentication**: QKD can be combined with other authentication primitives to perform message authentication function, e.g., universal-II hash functions, symmetric key based message authentication code (MAC);
- **Secret sharing**: QKD can be combined with Shamir's secret sharing algorithm to perform secure storage function;
- **Secure multi-party computation (SMC)**: QKD raw key can be used to implement oblivious key transfer to perform SMC;
- **Public key cryptography (PKC)**: QKD can be combined with PKC including PQC to provide hybrid security guarantee.

2) UCC2: QKD integrated with various TCP/IP protocols

QKD can be integrated with TCP/IP protocols at various layers, e.g., PPP and MACSec protocol at MAC layer, IPSec protocol at network layer, TLS protocol at transport layer.

3) UCC3: QKDN deployed in various network topologies

QKDN can be deployed with various network topologies connected via either fibre or free-space channels, e.g., line or ring or star topology, fibre-based metropolitan access network, fibre-based inter-city backbone network, free-space satellite-ground or inter-satellite network.

4) UCC4: QKD with different user device categories

QKD can be applied in different terminal types with different integration level, e.g.,

- Fixed user device connected to a standalone QKD module;
- Fixed user device which integrates QKD module as an internal component;
- Wireless user device which consumes offline keys provided by QKDN;
- Wireless user device which integrates QKD module to consume online keys provided by QKDN.

5) UCC5: QKD integrated in various network forms

QKD can be integrated in various ICT network forms which require high security guarantee, e.g., 4G/5G, SDN/NFV-based, cloud computing, blockchain, TSN, service chain and other future network evolutions, e.g., SCION, quantum internet.

6) UCC6: QKD applied in different vertical sectors

QKD can be applied in various vertical sectors which require high level and long-term security, e.g., finance, government, health care, energy, telecom, critical infrastructure.

8 Use Cases

(Editor's Note) After reviewing the use cases from the FG-QIT4N in the Appendix, it's necessary to select QKDN related use cases in the context of networking technologies as the mandate of ITU-T SG13. Then, the selected use cases will be moved into this clause with details.

(Editor's Note) At the SG13 meeting (Geneva, 13 – 24 March 2023), the meeting has agreed to use the following use case template.

- **Use case ID**: e.g., UC-QKDN-00X.
- **Use case description**: presents a short summary, overall explanations for a use case including background, motivations, related technologies and target areas, if possible with a diagram.
- **Problem statement**: identifies problems and/or limitations related to the use case.
- **Technical considerations**: discusses various technical issues and challenges to solve problems and/or limitations identified.
  NOTE: Technology maturity: assesses the maturity of the key technical solutions required to address technical considerations above, e.g., Technology Readiness Level (TRL), etc.
- **Standardization considerations**: conducts gap analysis with existing standards (refer to Y.supp.QKDN-roadmap) and identifies relevant standardization items for quantum networks beyond QKDN including any suggestions for future standardization in line with ITU-T SG13 work scope.
- **Others**: 1) Benefits and impact to describe the benefits that the use case would bring, and the impact it would have when applied. 2) Application prospects to assess the relevant application areas and potential markets, etc.

Formatted: Font: Italic

Formatted: Font: Not Bold

Formatted: Indent: Left: 0.53", No bullets or numbering

Formatted: Font: Not Bold

Formatted: Font: Times New Roman, Not Bold

Formatted: Font: (Default) Times New Roman, Not Bold

Formatted: Font: Times New Roman, Not Bold

I.1 UCC1: QKD combined with other cryptographic primitives

As QKD has the important property of being universally composable (UC) [b-Renner], it implies that QKD can be composed with other UC protocols, resulting in a composed protocol that is also UC. Some examples are listed as below:

- One-time pad (OTP) encryption is the only encryption scheme for which information-theoretic security can be proven. It is thus natural to combine it with QKD. As a consequence, when keys established by QKD are used to perform OTP encryption, the resulting protocol is an unconditionally secure message transmission protocol [b-Alléaume].
- Another frequent use case is QKD combined with a symmetric encryption scheme such as AES. This combination is the one that is currently adopted by existing commercial QKD vendors. It provides a practical solution to realize point-to-point link encryption applications with frequent key exchange.
- QKD can also be integrated with message authentication primitives, as reported in the SECOQC network, which combines QKD with an efficient implementation of universal-2 hashing authentication [b-ETSI GS QKD 002].

In addition, QKD has the potential to be integrated with other cryptographic schemes to provide various security enhancement solutions, as detailed in the following use case descriptions.

I.1.1 UC-1-1: QKD combined with secret sharing

Use case description

UC-1-1 describes a distributed cloud archive for long term storage of digital data with advanced security and privacy guarantees.

QKD links, as well as other technical and cryptographic means, ensure that data can be securely transported to the involved cloud providers while its integrity and confidentiality remain protected against the storage providers, other tenants of the involved storage clouds and any other non-entitled third parties.

The data is distributed among several cloud storage providers in a way that it remains available even when some cloud providers are not reachable (the minimum number of required cloud providers de-pends on the employed configuration).

The end user may at any time decide to exchange one cloud provider for another, without any consent or action required from the cloud provider, in a way that no exploitable information remains at the cloud provider.

I.1.2 UC-1-2: QKD combined with secure multiparty computation (SMC)

Use case description

UC-1-2 consists of a service which enables quantum secure multiparty computation to perform private recognition of composite signals. The generation and distribution of quantum oblivious keys are the basis of this novel service. The quantum oblivious keys are generated from the raw keys of a QKD system.

For the sake of simplicity, only two entities, **A** and **B**, which are in possession of two private sequences, x_A and x_B are considered. **A** and **B** want to perform a composite signal analysis using x_A and x_B over a public database, such as a protein or genome DNA sequence database, **P**. A possible situation where the service is useful is the following: **A** and **B** want to know if both sequence x_A and x_B appear in the public sequence **P** within a certain distance but they do not want to reveal their own sequences (x_A and x_B). For this purpose, **A** and **B** need to evaluate a function to perform this analysis, but this function will operate with encrypted inputs, $\tilde{x}_A$ and $\tilde{x}_B$ and generate encrypted

outputs, $\tilde{y}_A$ and $\tilde{y}_B$. Both entities will be equipped with an encoder/decoder able to generate, $\tilde{x}_A$ from x_A and y_A from $\tilde{y}_A$, respectively, and the same for entity **B**, see Figure 8-1.

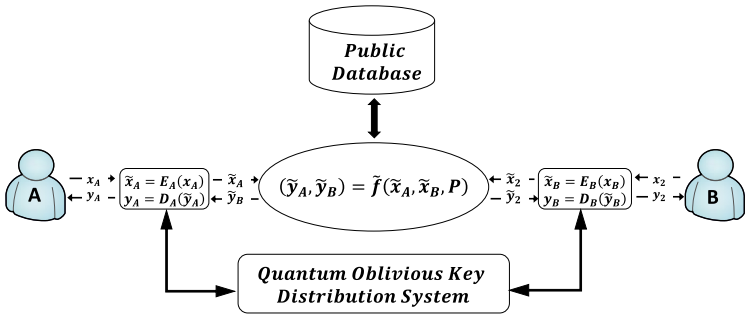

Figure 8-1 – Schema of the use case quantum enabled private recognition of composite signals

I.1.3 UC-1-3: Hybrid QKD and PQC for encrypted communications

Use case description

Quantum-safe cryptography is urgently needed to protect systems with high security requirements. Even though quantum computers are not available today, data can always be saved and decrypted later by quantum computers. A practical hybrid scheme with various quantum-safe technologies for encrypted communications between data centres has been demonstrated on Alibaba's platform [b-Leilei] to enhance data transfer security.

I.2 UCC2: QKD integrated with various TCP/IP protocols

As similar to the other key exchanging algorithms in cryptography, QKD can also be applied to the data link layer, network layer, transport layer, and application layer of the TCP/IP protocol stack which is commonly used in ICT systems, as shown in Figure 9-1.

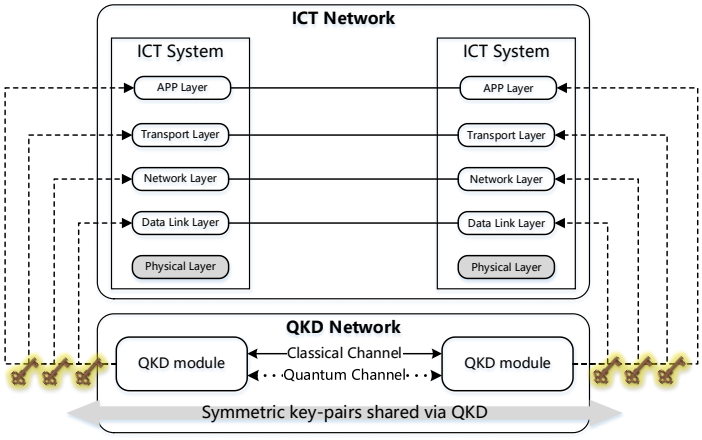

Figure 9-1 – QKDN integrated with TCP/IP protocol stack

I.2.1 UC-2-1: QKD integrated in data link layer

Use case description

On the data link layer, QKD may be used as a part of the point-to-point protocol (PPP) which is a layer 2 protocol widely used to connect two sets of nodes in a network. The encryption functionality in PPP is the encryption control protocol (ECP) [b-IETF RFC 1968]) which allows the use of encryption in PPP frames. QKD may be used as a key exchange protocol for PPP.

QKD may also be used to provide keys for the IEEE 802.1 MACsec layer 2 protocol which provides a connectionless service that supports data confidentiality, integrity and authenticity for authorized systems attaching to a local area network (LAN) or interconnecting LANs.

As QKD is presently mainly implemented as a point-to-point link involving two endpoints connected by a quantum channel, it is reasonable to combine a QKD link with a link encryptor to form a QKD link encryptor. A link encryptor is a network-transparent cryptographic system. A QKD link encryptor is a quantum cryptography appliance for point-to-point link encryption which may also be referred to as virtual private network (VPN) tunnel. The link encryptor usually uses the keys supplied by QKD as keys for a symmetrical block cipher (e.g., AES) or steam cipher (OTP for highest security) and can be used, for example, to encrypt traffic on an Ethernet of fibre channel link. The QKD link encryptor may be used to support communications between two adjacent network nodes employing QKD or it may provide protection for communications end-to-end across a network of nodes as a VPN tunnel. Key management is integrated in the link encryptor. For example, this solution may securely bridge two Fast Ethernet networks.

I.2.2 UC-2-2: QKD integrated in network layer

Use case description

Internet protocol security (IPsec) is a layer 3 protocol suite for securing internet protocol (IP) communications by authenticating and encrypting the IP packets of a data stream.

Internet key exchange (IKE or IKEv2) is the protocol used to set up a security association in the IPsec protocol suite. IKE uses a Diffie-Hellman public key exchange to set up a shared session secret, from which cryptographic keys are derived. Public key techniques or, alternatively, a pre-shared key, are used to mutually authenticate the communicating parties.

QKD may be used by a modified IKE protocol to provide the shared secret for IPsec payload encryption. The shared secret provided by QKD may either be used in a conventional block or stream cipher for OTP payload encryption in a high security context.

I.2.3 UC-2-3: QKD integrated in transport layer

Use case description

Transport layer security (TLS) and its predecessor secure sockets layer (SSL) are layer 4 protocols which provide an end-to-end security for network communication services. A session key, usually established with public key exchange, is used e.g., to secure the transmission of credit card information in e-commerce transactions. In a scenario involving QKD, the session key may be replaced by a QKD key or the QKD keys may immediately be used for OTP encryption of transmission data. QKD keys may also be used for message authentication, replacing hash-based message authentication codes (HMACs) as used in TLS, or the pseudo-random functions of standard SSL.

I.2.4 UC-2-4: QKD integrated in application layer

Use case description

Above the transport layer, QKD systems may be integrated in layer 7, the application layer of the OSI model. This may be useful for applications using pre-shared keys for user authentication or for the acquisition or certain rights, or as encryption keys for payload transmission between instances of the application.

I.3 UCC3: QKD implemented in various network topologies

I.3.1 UC-3-1: QKDN as metropolitan access network

Use case description

UC-3-1 describes a general-purpose high security communications network between several branches and offices within an area of about 100 km in diameter (metropolitan area). The single network nodes are interconnected with dedicated optical point to point links for classical digital communication and QKD. The network uses a dedicated optical infrastructure which is completely separated from the internet.

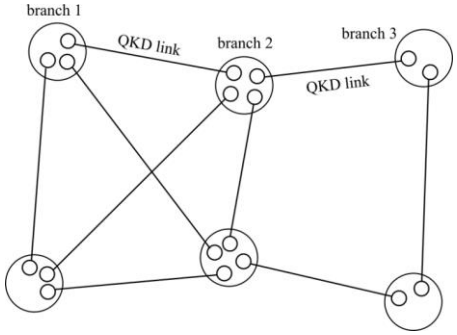

Figure 10-1 – High security metropolitan area network topology

QKD systems are used to generate symmetrical secrets in nodes connected by optical links. The secrets are used as cryptographic keys for authentication and encryption primitives with security levels fitting the purpose they are intended for. Provably secure OTP can be used for communications with strictest long term security requirements, while other algorithms, including PQC algorithms can also be used. To increase network connectivity (between links without direct connection), and availability and/or bandwidth, a trusted repeater network solution can also be considered.

(Editor's Note) From C-077 (Q16/13 e-meeting, 11-16 January 2023), the following use case on distributed quantum computing has been added.

8.1 QKDN as metropolitan access network

8.1.2 Problem statement

Governments and other organizations with the highest communications security requirements are currently relying on communication networks which either use dedicated network infrastructures or are layered upon the internet. In both cases, cryptography is used with an uncertain prospect with regards to current and especially long-term security.

Current cryptographic protocols and paradigms have already been subject to severe (mostly insider) attacks. Examples of such attacks include compromised random number generators making brute forcing TLS keys a trivial task, compromised root certificates for trust validation, etc. Some algorithms for securing governments' communication shave later turned out to have contained deliberately introduced weaknesses; even AES is suspected to be susceptible to timing side channel attacks. Furthermore, in most jurisdictions, COTS telecom and network hardware, e.g., network switches are required by legislation to include access mechanisms for law enforcement which have already been exploited by rogue actors. With regards to long term security, the prospects are even worse: secrets that need to remain secure for several decades may be revealed some time in the future when advanced decryption capabilities including quantum computers become available.

8.1.3 Solution

The solution would be to use a communications network with advanced security guarantees on a dedicated optical infrastructure that is completely separated from the internet. The advanced security is provided by QKD links delivering a continuous stream of symmetrical secrets used to authenticate and secure the communication between adjacent nodes of the network. To increase network availability and/or bandwidth, a trusted repeater network solution may also be considered.

I.3.2 UC-3-2: QKDN as inter-city backbone network

Use case description

In September 2017, the 2000 km Beijing-Shanghai backbone QKD network was put into operation and, at the time of this report's publication, was the longest QKD network in the world. The project was led by the University of Science and Technology of China (USTC) in partnership other with organizations including China Cable Television Network Co., Ltd, Shandong Academy of Information & Communication Technology, Industrial and Commercial Bank of China (ICBC), Xinhua Financial Information Exchange etc.

The backbone network consists of 32 physical nodes linearly connected by QKD links – the Beijing, Jinan, Fuli, Hefei, Nanjing and Shanghai nodes are the access points while the others are trusted repeater nodes. The backbone network has 135 links in total and two to eight multiple QKD links lie between adjacent nodes. The network rents dark fibres deployed by China Cable Television Network Co., Ltd. and, to conserve fibre resources, the network uses quantum wavelength division multiplexing technology which combines four quantum channels into a single fibre. The distance between adjacent nodes along the backbone line varies between 34 km and 89 km with fibre loss varying from 10.3 dB to 20.5 dB.

The backbone network deploys QKD devices (provided by QuantumCTek Co., Ltd) which implement decoy state BB84 protocol. Some of the devices integrate the up-conversion single photon detection technique and thereby achieve a 25% single photon detection rate.

The backbone network is designed to function as a high bandwidth channel that feeds quantum keys between metropolitan and QKD networks located in different cities. The backbone network has been connected to four metropolitan QKD networks already established in Beijing, Shanghai, Jinan and Hefei. A wide area QKD network thus has been formed and provides end users including banks, government agencies and large enterprises with versatile security services, such as video call, audio call, fax, text transmission and file transmission. The network is also scalable such that extra users can be easily added.

I.3.3 UC-3-3: QKDN as free-space satellite-ground or inter-satellite network

Use case description

UC-3-3 describes a high security general-purpose long-haul network based on multi-layer satellites around the world. By using satellite as relay, long-distance QKD can be realized within global metropolises.

As shown in Figure 10-2, general-purpose long-haul network based on multi-layer satellites consists of three layers of geostationary earth orbit (GEO) satellite, medium earth orbit (MEO) satellite and low earth orbit (LEO) satellite. The multi-layer satellite in orbit provides the physical basis for the application of general-purpose long-haul network.

The general-purpose long-haul network based on multi-layer satellites can cover the whole world through satellite communication with flexible user access. It is suitable for remote areas with high cost of laying optical fibre to realize quantum key distribution. At the same time, it can solve the

problem of difficult access for mobile users, such as marine mobile equipment, polar research station, desert detection station, etc.

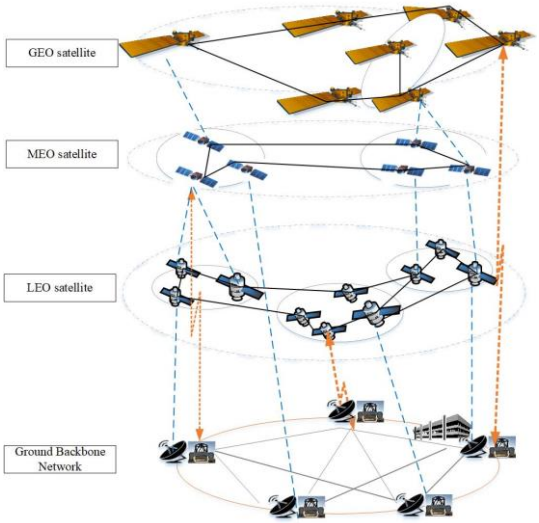

Figure 10-2 – Architecture of general-purpose long-haul network based on multi-layer satellites

Simpler satellite-based QKD networks, e.g., single layer satellite based QKDNs, may be less robust and produce less QKD keys but might still be adequate for some commercial and lower security applications.

I.4 UCC4: QKD with different user device categories

From a QKD end user's perspective, there are various use cases according to the different types of user devices consuming the keys provided by QKDN. The possible use cases include:

– **Fixed user device with standalone QKD module**: As current commercial QKD devices are typically bulky and require a fibre connection, the user devices placed at a user's office such as the router, the encryptor and the QKD devices are usually separate devices as shown in Figure 11-1. The encryptor connects to the QKD device with a physical connection to fetch keys and then encrypts or decrypts the data traffic passed in the router.

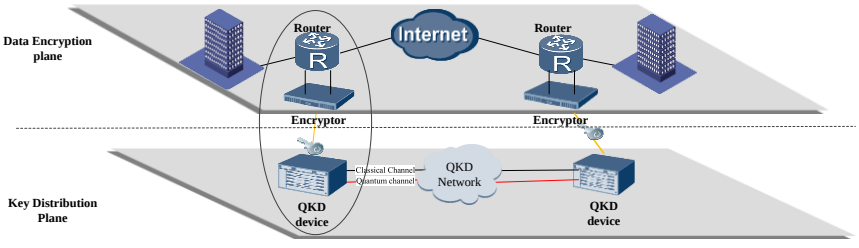

Figure 11-1 – QKD used via fixed user device with standalone QKD module

– **Fixed user device with integrated QKD module**: As the QKD module integration level grows, the functionality of QKD can be integrated into a router or encryptor device physically as a chipset or a PCI card.

– **Wireless user device which consumes offline keys provided by QKDN**: For a wireless user device without a fibre connection to the QKDN, it can store the keys provided by QKDN into the secure storage within itself and then consume the keys for secure data communication as shown in Figure 11-2. The detailed use case description is provided in UC-4-1.

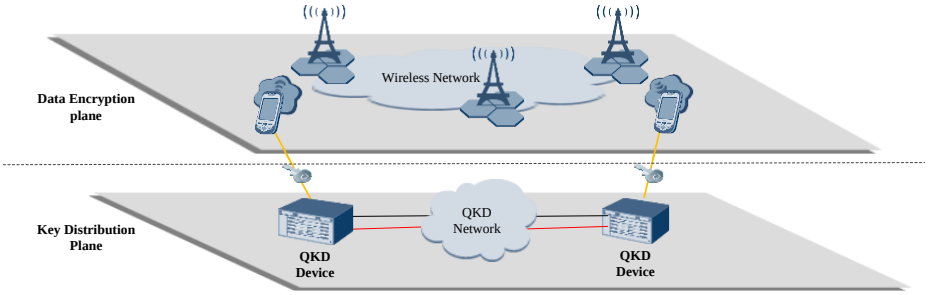

Figure 11-2 – QKD used via wireless user device with offline QKD-keys

– **Wireless user device which integrates a QKD module to consume online keys provided by QKDN**: As wireless and mobile QKD technology is developing, it is also possible to integrate QKD module into wireless devices and perform QKD directly via wireless channels. More details on this use case are provided in UC-4-2.

I.4.1 UC-4-1: Wireless user device with offline QKD-keys

Use case description

In UC-4-1, the proposed solution is to pre-install the QKD-key pool into the mobile user and network side to enhance security of mobile communication which is achievable with existing QKD techniques.

I.4.2 UC-4-2: Wireless user device with integrated QKD module

Use case description

As the QKD module can be miniaturized into chip-scale, it is possible to be integrated into mobile devices to perform wireless QKD service. As shown in Figure 11-4, the University of Bristol in the United Kingdom has successfully demonstrated the QKD chip transmitter integrated on the credit card, and the QKD receiver in the ATM rack to achieve free-space QKD.

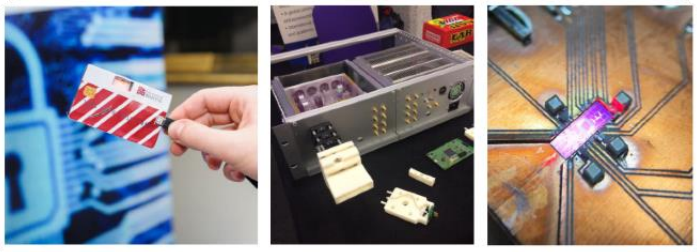

Figure 11-5 – Demo of QKD integrated credit card

I.5 UCC5: QKD integrated in various network forms

I.5.1 UC-5-1: QKD in 4G/5G networks

UC-5-1-1: QKDN for LTE backhaul and 5G backbone

Use case description

The first commercial QKD network in Korea (Rep. of) was deployed in June 2016. This network applied QKD to LTE backhaul between Sejong central office and one of SK telecom's DU site at Daejeon.

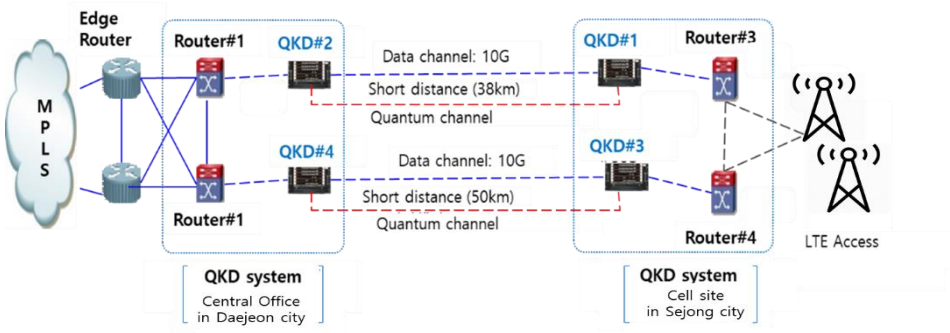

Figure 12-1 – QKD network deployment in LTE backhaul in Korea

In 2017, a trusted relay node was implemented for long distance QKDN and in 2019, the implementation and commercialization of QKD quantum cryptography for a total of 221 km of transmission line between Sungsu central office (Seoul area) and Dunsan central office (Daejeon area) of SK Telecom was accomplished. It was extended to the Taepyung central office in 2020 and this is the end-to-end distance of 380 km. Other main cities are targeted to be reached with QKD step by step.

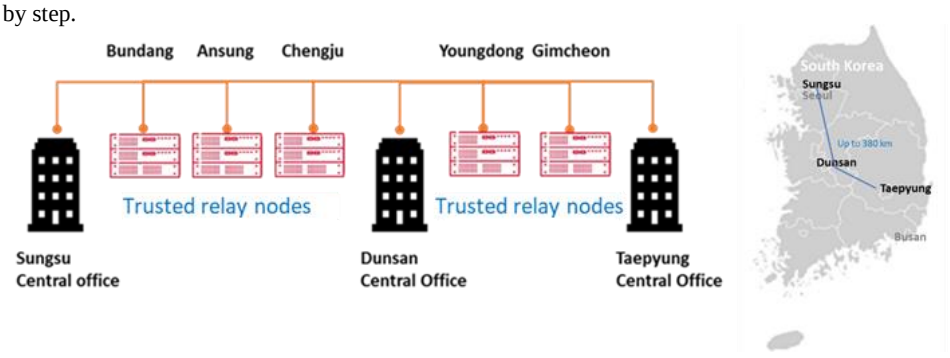

Figure 12-2 – Long distance QKD network deployment in LTE and 5G backbone in Korea

UC-5-1-2: Quantum secured inter-domain 5G service orchestrator

Use case description

In [b-Wang], it is reported that QKD technologies in combination with SDN and network function virtualization (NFV) can be applied to secure interconnections of distributed virtual network functions (VNFs) to achieve quantum secured inter-domain 5G service orchestration.

This was experimentally demonstrated via interconnecting four autonomous 5G islands simultaneously through the q-ROADM with eight optical channels using the 5GUK Exchange orchestration platform. The overall concept is as shown in Figure 12-3 [b-Wang].

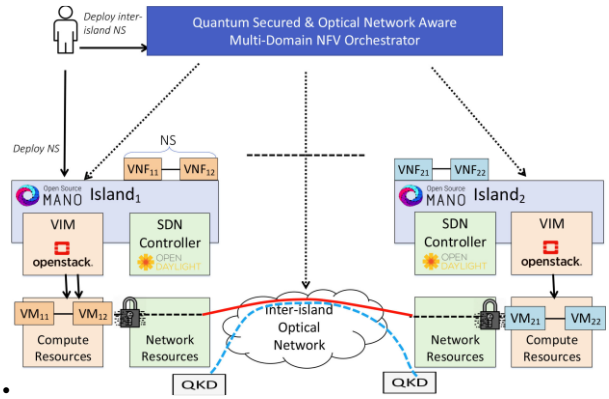

Figure 12-3 – Overall concept of QKD secured 5GUK Exchange scenario

UC-5-1-3: QKDN for 5G front-haul

Use case description

For 3G/4G networks, the base station (or known as eNodeB by 3GPP) is comprised of the base band unit (BBU) and the remote radio unit (RRU). The front-haul is referred to as the fibre connection between the BBU and RRU which features a high bandwidth, low latency and private CPRI interface.

For 5G, the base station (or known as gNodeB by 3GPP) functions are reallocated into three parts as RRU, distributed unit (DU) and central unit (CU), as shown in Figure 12-4.

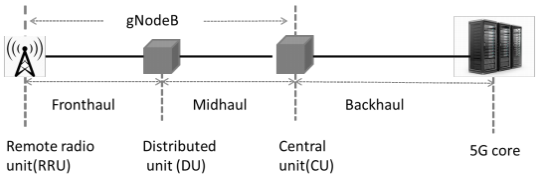

Figure 12-4 – 5G transport structure

The 5G RRU can handle certain physical layer functions of previous BBU locally, thus, the fronthaul transportation requirements can be relaxed to accommodate the surging 5G capacity. The next generation fronthaul interface (NGFI) is designed for the connection between RRU and DU, as a new decoupled open interface to support RRU and DU from different vendors.

The security guarantee for 5G fronthaul is an important issue which need to satisfy high bandwidth, low latency and high-level security at the same time.

QKD is a promising solution to secure 5G fronthaul which is mentioned in [b-Priem].

UC-5-1-4: QKDN for 5G mid-haul

Use case description

The mid-haul is a newly introduced concept in 5G to indicate the connection between the DU and CU.

SK Telecom (SKT) has showcased the application of QKD to the 5G mid-haul network to secure confidential data transmission from a smart factory to the cloud.

A customer of SKT, an auto parts manufacturer (Myunghwa Industry) based in Ansan, implemented a smart factory using IoT devices and robots which generates a large volume of confidential data such as design documents transmitted over the 5G network to reach the SKT Cloud. Therefore, the customer was looking for fast and secure access to the SK Telecom commercial 5G service to connect their new smart factory.

To best address this customer security need, SKT has secured the 5G network connectivity with the latest quantum safe technology using quantum cryptography. One 5G DU is located on the SKT's customer site in Ansan while the 5G CU is located at the central office of SKT Network in Sungsoo. Since the 5G DU to CU connectivity uses a fibre optic network, it was possible to combine QKD with the encryption on the 5G mid-haul network. The deployment is illustrated in Figure 12-5.

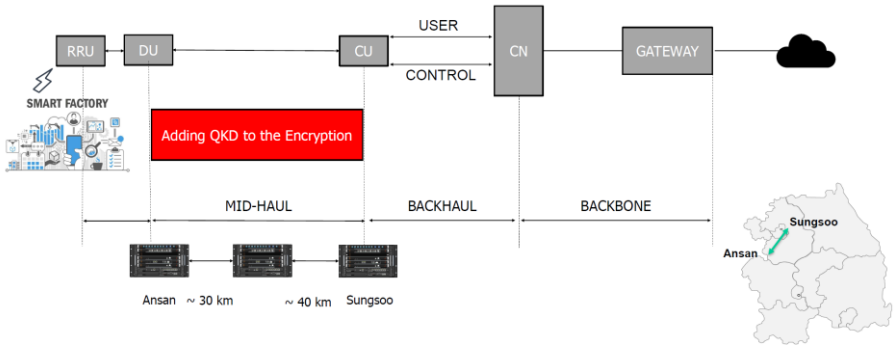

Figure 12-5 – 5G mid-haul QKD deployment for smart factory

This solution combines the latest technology available ensuring high-speed, stability and security for the customer data connectivity.

UC-5-1-5: Quantum security enhancement for universal AKA authentication protocol

Use case description

Authentication verifies whether a user has the right to access a system. In the traditional authentication mode, users present valid information such as passwords to the authentication party to verify that they have the right to access the system. Authentication includes user authentication and network authentication where:

- user authentication means that the network authenticates users to prevent unauthorized users from occupying network resources; and
- network authentication allows users to authenticate networks to prevent users from accessing illegal networks and obtaining key information.

The Authentication and Key Agreement (AKA) is a two-way authentication mechanism defined in [b-RFC4187]; its improved version AKA' is defined in [b-RFC5448]. Both mechanisms have been

developed by IETF and adopted by 3GPP and are widely used wireless network authentication mechanisms.

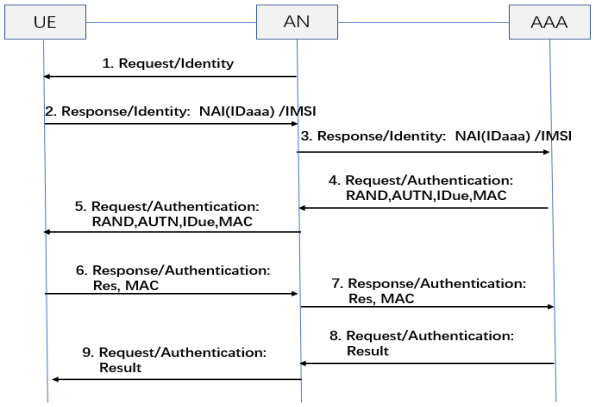

Figure 12-6 – AKA authentication protocol

12.1.6 UC-5-1-6: Secondary authentication protocol in 5G based on quantum security

Use case description

Network slices have been introduced in 5G to meet the differentiated needs of different industries. To prevent unauthorized users from accessing the industry's network slices, 5G proposes secondary authentication for user access. The secondary authentication refers to the authentication between the end user and the data network outside the ISP's domain so that legitimate users can have secure access to the data network. According to [b-3GPP TS 33.501], the secondary authentication process applies between the user terminal, UE and the AAA server of the external data network (DN). The authentication protocol is based on the EAP framework defined in [b-RFC3748] and can be customized.

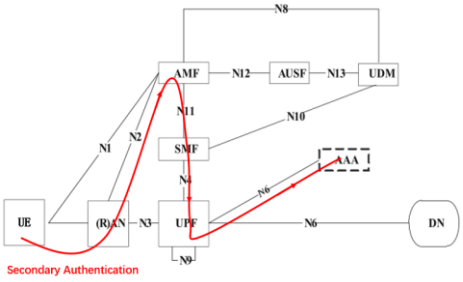

Figure 12-8 – Secondary authentication protocol in 5G

UC-5-1-6 describes two newly designed schemes quantum secure symmetrical encryption (EAP_QSSE) and quantum secure symmetrical encryption and hash-function (EAP_QSSEH) based on quantum security. Both authentication parties use quantum random numbers as authentication factors and QKDN to share keys, for two-way authentication of UE and AAA, to achieve lightweight and fast 5G network secondary authentication in a symmetrical encryption authentication manner.

Figure 12-9 – Secondary authentication protocol based on quantum security

I.5.2 UC-5-2: QKD in SDN/NFV based network

UC-5-2-1: Secure SDN and NFV control and management plane

Use case description

The implementation of UC-5-2-1 involves the creation of QKD keys that are combined with the usual keys in the protocols used so that the security is incremental: to break into the system, the old protocols have to be broken but also the new QKD layer.

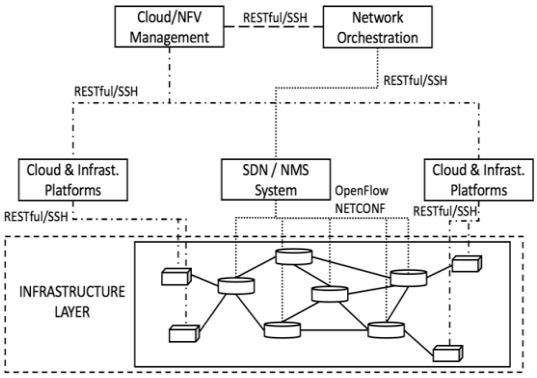

Figure 12-10 – Abstract view of a control plane architecture including cloud/NFV and network orchestration and SDN control plane to secure by QKD

A diagrammatic description of the testbed used to implement UC-5-2-1 in 2018 is depicted in Figure 12-11 with only two transponders and up to 17 classical co-propagating channels were used together with the quantum channel.

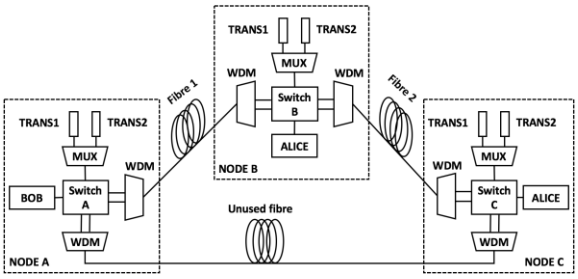

Figure 12-11 – Diagrammatic description of the testbed used to implement the use-case in 2018

UC-5-2-2: Quantum encryption for end-to-end services

Use case description

UC-5-2-2 combines QKD systems to secure end-to-end (E2E) services e.g., transport tunnels, VPNs between remote premises. Protocols like patch computation element protocol (PCEP) and multiprotocol label switching (MPLS) are used and modified to use QKD.

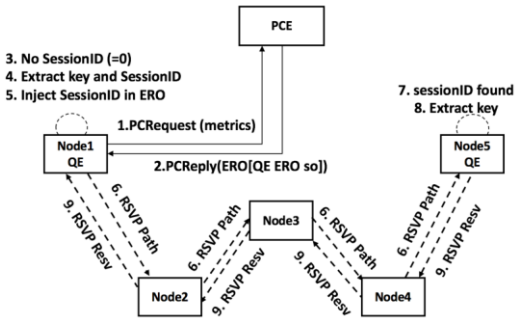

Figure 12-12 – MPLS/PCEP workflow for setting up a quantum encryption service

Figure 12-13 illustrates a logical scheme describing the network used for the E2E quantum encryption service via IPsec. The left part shows the DC management and data networks, with a QKD domain (Bob) and a virtual router connected to a PCE while the right part shows the local network connecting another virtual router to the remote PCE and another QKD domain (Alice). The intermediate area exposes the packet/optical network.

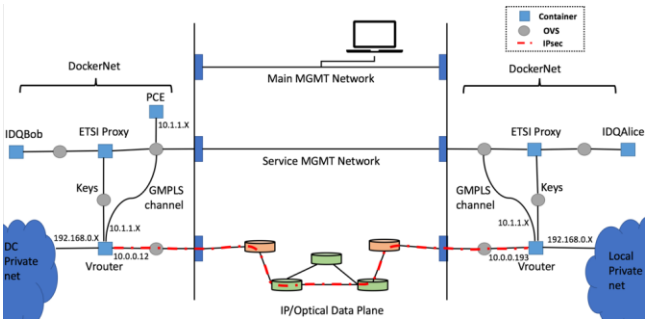

Figure 12-13 – Logical scheme describing the network used for the E2E quantum encryption service via IPsec

UC-5-2-3: Quantum security for service chaining

Use case description

A proof-of-transit technique has been developed to verify if a packet has traversed all the nodes within a path. QKD is used to provide order to the proof of transit as well as security enhancement. Figure 12-14 illustrates a representation of an ordered proof of transit scheme in a network. The input and output nodes are connected by a chain of nodes that each packet must travel.

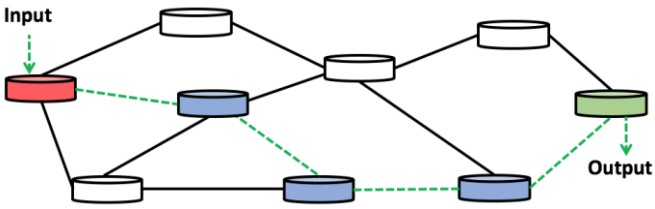

Figure 12-14 – Representation of an ordered proof of transit (OPoT) scheme in a network

Figure 12-15 illustrates the setup for the ordered proof of transit to secure service chaining as it was used in the Madrid quantum network [b-Aguado-3]. Two logical layers are shown: the QKD layer (lower part) and the data, OPoT layer (upper part).

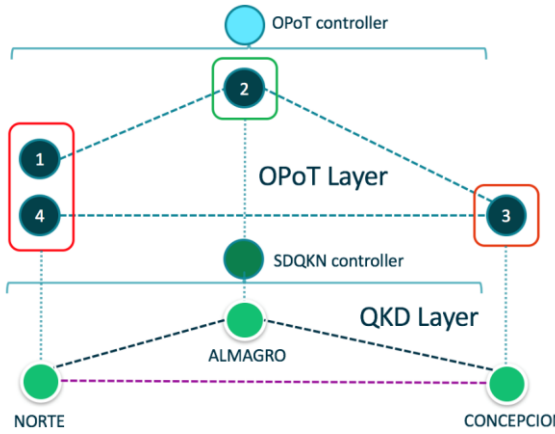

Figure 12-15 – OPoT-DEM: setup for the ordered proof of transit to secure service chaining as was used in the Madrid quantum network

I.5.3 UC-5-3: QKD in blockchain network

UC-5-3-1: Quantum-secured blockchain

Use case description

[b-Kiktenko] proposes a quantum-safe blockchain solution based on QKD.

UC-5-3-2: Quantum vault for blockchain

Use case description

In [b-Huttner], ID Quantique and its partners propose a quantum vault solution to utilize QKD and QRNG to enhance the security of blockchain.

I.5.4 UC-5-4: QKD in TSN network

Use case description

The time-sensitive networking (TSN) is one widely applied communication standard developed by IEEE to meet stringent latency and timing requirements of the industrial environment.

Ensuring cybersecurity is also an important requirement in life-critical control systems for which industrial TSN will provide communication. While private key exchange which requires manually pre-sharing keys and public key exchange which requires more computing resources are discouraged for the TSN targeted scenario, QKD can be one possible solution for TSN, as manifested in [b-Avnu].

I.5.5 UC-5-5: QKD in SCION

Use case description

Despite the fast advancement of internet-based services, the architecture and core protocol have remained mostly the same for decades since the internet's inception. However, to accommodate the ever increasing and diverse data services more efficiently and securely, a new architecture is necessary and several efforts have been made for a next-generation internet architecture. QKD can play an important role in a new internet architecture to enhance the security, which is one of the main concerns that today's internet is facing.

One example use case introduced here is the QKD integration with Scalable, Control and Isolation on Next-Generation Networks (SCION) which is a research project led by researchers at ETH Zurich. SCION aims to offer a communication infrastructure that remains highly available even in the presence of adversaries.

Some typical vertical applications of QKD in SCION include for high-availability communication such as financial networks and industrial control systems used for power distribution. Governments can also use this architecture for critical communication infrastructure such as law enforcement communication.

Achievable security levels: A network is considered secure if it can achieve the desired properties even in the presence of an active adversary. One such prominent property is availability, i.e., the control-, data-, management-, and configuration-planes should be protected such that an adversary cannot disrupt basic communication connectivity.

I.6 UCC6: QKD applied in different vertical sectors

QKD can be applied in various vertical economic sectors that require high level and long-term security which may include, but are not limited to, the following:

- Finance
- Government and public sectors
- Healthcare, e.g., to secure genome data
- Telecom networks, e.g., to secure 5G network
- Industry networks
- Other critical infrastructures

I.6.1 UC-6-1: QKDN for smart factory

Use case description

Hyundai Robotics manufactures industrial robots, applies them to overseas industrial facilities and remotely operates through various ICT infrastructure such as IoT devices, leased line and servers. In this process, a malicious hacking threat on optical cable of leased line may cause production disruption due to confidential leaks.

To prevent such problems, a commercial QKDN for the smart factory has been installed to protect corporate information and to enhance security. This network applies QKD to leased line between Hyundai Robotics and KT Corp. office in Daegu, see Figure 13-1 for an illustration.

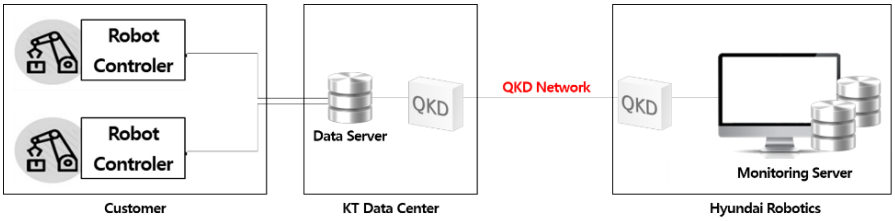

Figure 13-1 – QKDN for smart factory

I.6.2 UC-6-2: QKDN for social safety

Use case description

Local governments operate drone-based surveillance system for public safety. In particular, since it is necessary to be careful about information leakage in areas adjacent to military camps, QKD networks are applied to drone communication.

Korea (Rep. of) is deploying a commercial QKDN for social safety and this network applied QKD for drone communication between two adjacent local governments in Gangwon-do, see Figure 13-2.

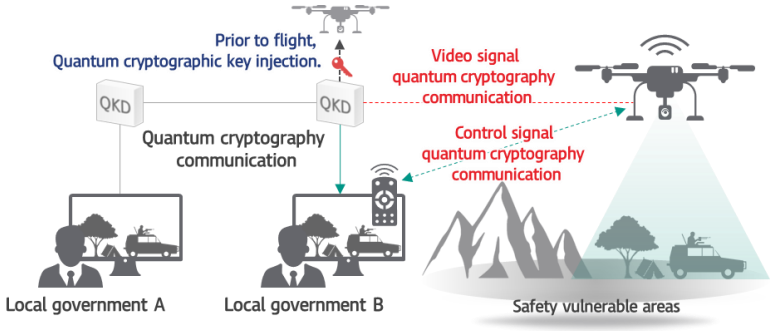

Figure 13-2 – QKDN for social safety

By injecting the quantum encryption key supplied from QKD into the drone, not only is the drone control signal protected, but also the video signal from the drone is encrypted and protected to improve security.

I.6.3 UC-6-3: QKDN for medical centre

Use case description

In St. Mary's Hospital, a large medical institution in Korea (Rep. of)., the central medical data server manages the medical data of branches located in various regions and the branches share medical data such as patient information and medical records through the central medical data server. In this sharing process, there is a possibility that medical information, which is personally sensitive information, may be leaked by hacking.

To prevent such threats, a commercial QKDN has been applied between medical data servers to encrypt medical data and improve security. This network applied QKD to leased line between St. Mary's Hospitals and their data centre in Seoul, see Figure 13-3.

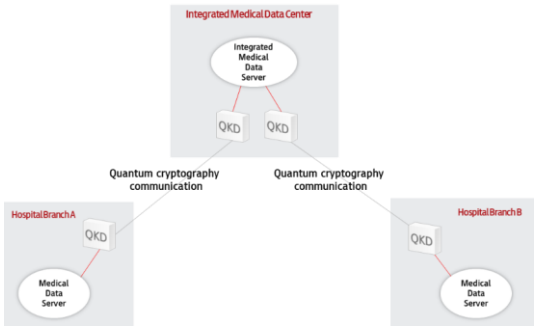

Figure 13-3 – QKDN for medical centre

I.6.4 UC-6-4: QKDN for secure mVoIP

Use case description

For mVoIP, there are threats of hacking such as voice terminal wiretapping, voice network wiretapping, and session hijacking attack. To prevent such threats, a commercial QKDN for secure mVoIP was deployed in Korea (Rep. of). This network applies QKD to VoIP communication between two smart phones, see Figure 13-4.

The KSA key is received from the QKDN and injected into the secure communication devices and the mVoIP voice call data is encrypted through the devices.

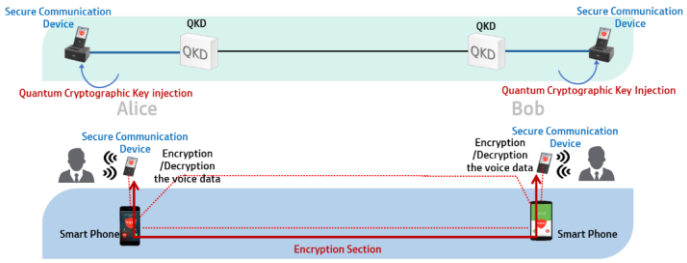

Figure 13-4 – QKDN for secure mVoIP

Appendix I

Overview of QKDN use cases

(Editor's Note) This Appendix is the collection of QKDN use cases as the result of FG-QIT4N. New use cases can be identified and reviewed. Contributions are invited.

This Appendix provides an overview of the QKDN use cases considered by the Focus Group on Quantum Information Technology for Networks.

To select related use cases, the following table has been made to show use cases in the FG-QIT4N deliverable D2.2 (Appendix of Y.supp.QKDN-UC) and related SG.

Use cases	Related SG
I.1 UCC1: QKD combined with other cryptographic primitives	
I.1.1 QKD combined with secret sharing	SG13, SG17
I.1.2 QKD combined with SMC	SG13, SG17
I.1.3 Hybrid QKD and PQC for encrypted communications	SG13, SG17
I.2 UCC2: QKD integrated with various TCP/IP protocols	
I.2.1 QKD integrated in data link layer	SG13
I.2.2 QKD integrated in network layer	SG13
I.2.3 QKD integrated in transport layer	SG13
I.2.4 QKD integrated in application layer	SG13
I.3 UCC3: QKD implemented in various network topologies	
I.3.1 QKDN as metropolitan access network	SG13
I.3.2 QKDN as inter-city backbone network	SG13
I.3.3 QKDN as free-space satellite-ground or inter-satellite network	SG13
I.4 UCC4: QKD with different user device categories	
I.4.1 Wireless user device with offline QKD-keys	(SG13)
I.4.2 Wireless user device with integrated QKD module	(SG13)
I.5 UCC5: QKD integrated in various network forms	
I.5.1 QKD in 4G/5G networks	SG13
I.5.2 QKD in SDN/NFV based network	SG13
I.5.3 QKD in blockchain network	SG13
I.5.4 QKD in TSN network	SG13
I.5.5 QKD in SCION	SG13
I.6 QKD applied in different vertical sectors	
I.6.1 QKDN for smart factory	(SG13)
I.6.2 QKDN for social safety	(SG13)

I.6.3 QKDN for medical centre	(SG13)
I.6.4 QKDN for secure mVoIP	(SG13)

I.1 UCC1: QKD combined with other cryptographic primitives

I.1.1 QKD combined with secret sharing

Use case ID	UC-1-1
Short description	This use case describes a distributed cloud archive for long term storage of digital data with advanced security and privacy guarantees. QKD links, as well as other technical and other cryptographic means ensure that the data can securely be transported to the involved cloud providers, and remains integrity protected, as well as confidentiality protected against the storage providers, other tenants of the involved storage clouds, as well as other non-entitled third parties.

I.1.2 QKD combined with SMC

Use case ID	UC-1-2
Short description	This use case describes quantum enabled private recognition of composite signals in proteins and genome. It consists of a service which enables quantum secure multiparty computation to perform private recognition of composite signals. The generation and distribution of quantum oblivious keys are the basis of this novel service. The quantum oblivious keys are generated from the raw keys of a QKD system. This use case is based on use cases UC-5-2-1 and UC-5-2-2.

I.1.3 Hybrid QKD and PQC for encrypted communications

Use case ID	UC-1-3
Short description	Quantum-safe cryptography is urgently needed to protect systems with high security requirements, as data today can be saved and decrypted later by quantum computers. Both QKD and PQC present opportunities and obstacles. QKD can provide provably-random keys and information theoretic secure distribution of those keys. However, to deploy a QKD system in the real-world, the technology must overcome the transmission distance problem as well as restrictions of point-to-point links, high manufacturing and maintenance cost, and lack of scalability. PQC, on the other hand, is similar to classical cryptography that is algorithm-based. However, deploying a new cryptosystem incurs potentially high cost, with the time and energy consumed by cryptographic computations. In addition, PQC in principle still faces the risk of potential attacks by future mathematical breakthroughs. QKD and PQC can be integrated in the hybrid quantum-safe scheme to enhance data transfer security.

I.2 UCC2: QKD integrated with various TCP/IP protocols

I.2.1 QKD integrated in data link layer

Use case ID	UC-2-1
Short description	On the data link layer, QKD may be used as a part of the Point-to-Point Protocol (PPP) protocol. The encryption functionality in PPP is the Encryption Control Protocol (ECP - RFC 1968) which allows the use of encryption in PPP frames. QKD may be used as a key exchange protocol for PPP. QKD may also be used to provide keys for the IEEE 802.1 MACsec layer 2 protocol. As QKD is today mainly implemented as point-to-point link involving two endpoints

	connected by a quantum channel, it is reasonable to combine a QKD link with a link encryptor to form a QKD link encryptor. Key management is integrated in the link encryptor. For example, this solution may securely bridge two Fast Ethernet networks.

I.2.2 QKD integrated in network layer

Use case ID	UC-2-2
Short description	QKD may be used by a modified IKE protocol to provide the shared secret for IPsec payload encryption. The shared secret provided by QKD may either be used in a conventional block or stream cipher for One-Time-Pad payload encryption in a high security context.

I.2.3 QKD integrated in transport layer

Use case ID	UC-2-3
Short description	Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are layer 4 protocols, which provide end-to-end security for network communication services. A session key, usually established with public key exchange, is used e.g. to secure the transmission of credit card information in e-commerce transactions. In a scenario involving QKD, the session key may be replaced by a QKD key, or the QKD keys may immediately be used for One-Time-Pad encryption of transmission data. QKD keys may also be used for message authentication, replacing Hash-based Message Authentication Codes (HMACs) as used in TLS, or the pseudo-random functions of standard SSL.

I.2.4 QKD integrated in application layer

Use case ID	UC-2-4
Short description	Above the transport layer, QKD systems may be integrated in layer 7, the application layer of the OSI model. This may be useful for applications using pre-shared keys for user authentication or for the acquisition or certain rights, or as encryption keys for payload transmission between instances of the application.

I.3 UCC3: QKD implemented in various network topologies

I.3.1 QKDN as metropolitan access network

Use case ID	UC-3-1
Short description	This use case describes a general-purpose high security communications network between several branches and offices within an area of about 100km in diameter (metropolitan area). The single network nodes are interconnected with dedicated optical point to point links for classical digital communication and quantum key distribution. The network uses a dedicated optical infrastructure, which is completely separated from the internet.

I.3.2 QKDN as inter-city backbone network

Use case ID	UC-3-2
Short description	In September 2017, the 2000 km Beijing-Shanghai backbone QKD network was put into operation. The backbone network consists of 32 physical nodes linearly connected by QKD links and has 135 links in total. Two to eight multiple QKD links lie between adjacent nodes. The backbone network is designed to function as a high bandwidth channel that feeds quantum keys between metropolitan and QKD networks located in different cities. The backbone network has been connected to four metropolitan QKD networks already established in Beijing, Shanghai, Jian and Hefei.

I.3.3 QKDN as free-space satellite-ground or inter-satellite network

Use case ID	UC-3-3
Short description	This use case describes a high security general-purpose long-haul network based on multi-layer satellites around the world. By using satellite as relay, long-distance QKD can be realized within the global metropolises.

I.4 UCC4: QKD with different user device categories

I.4.1 Wireless user device with offline QKD-keys

Use case ID	UC-4-1
Short description	This use case describes QKD-key embedded secure mobile communication. To extend QKD service to the mobile terminals is envisioned with high value, but the current physical layer limitations still restrict the direct application of QKD via the air interface between mobile user equipment and base stations. In this use case, the proposed solution is to pre-install the QKD-key pool into the mobile user and network side to enhance security of mobile communication which is achievable with existing QKD techniques.

I.4.2 Wireless user device with integrated QKD module

Use case ID	UC-4-2
Short description	As QKD module being miniaturized into chip-scale, it is possible to be integrated into mobile devices to perform wireless QKD service. This use case describes a successful demonstration, by the University of Bristol in the United Kingdom, of the QKD chip transmitter integrated on the credit card, and the QKD receiver in the ATM rack to achieve the free-space quantum key distribution.

I.5 UCC5: QKD integrated in various network forms

I.5.1 QKD in 4G/5G networks

I.5.1.1 QKDN for LTE backhaul and 5G backbone

Use case ID	UC-5-1-1
Short description	This use case describes a network applying QKD to LTE backhaul between Sejong central office and one of SK Telecom's DU site at Daejeon. A trusted relay node was implemented for long distance QKD networks in 2017. Implementation and commercialization of QKD quantum cryptography for a total of 221km of transmission line between Sungsu central office (Seoul area) and Dunsan central office (Daejeon area) of SK Telecom was accomplished in 2019. It will be extended to Taepyung central office and this will make the end to end distance 380km. Other main cities will be reached with QKD step by step.

I.5.1.2 Quantum secured inter-domain 5G service orchestrator

Use case ID	UC-5-1-2
Short description	This use case describes QKD technologies in combination with SDN and NFV and their application in securing interconnections of distributed VNFs to achieve quantum secured inter-domain 5G service orchestration.

	And it was experimentally demonstrated via interconnecting four autonomous 5G islands simultaneously through the q-ROADM with eight optical channels using the 5GUK Exchange orchestration platform.

I.5.1.3 QKDN for 5G front-haul

Use case ID	UC-5-1-3
Short description	The security guarantee for 5G fronthaul is an important issue which need to satisfy high bandwidth, low latency and high-level security at the same time. QKD is a promising solution to secure 5G fronthaul and this use case describes the application of QKD to secure the 5G fronthaul.

I.5.1.4 QKDN for 5G mid-haul

Use case ID	UC-5-1-4
Short description	The mid-haul is one newly introduced concept in 5G to indicate the connection between DU (Distributed Unit) and CU (Centralized Unit). SK Telecom has showcased the application of QKD to the 5G mid-haul network, in order to secure the confidential data transmission from a smart factory to the cloud. This use case describes how SKT has secured the 5G network connectivity with the latest quantum safe technology using quantum cryptography to best address a customer's security need. This solution combines the latest technology available ensuring high-speed, stability and security for the customer data connectivity.

I.5.1.5 Quantum security enhancement for universal AKA authentication protocol

Use case ID	UC-5-1-5
Short description	QKDN is used to realize the advantage of secure key distribution. The client UE and the authentication server AAA use QKDN to share keys. Symmetric encryption fully ensures the security of data. The quantum random number generator (QRNG) can generate enough secure true random numbers for the client and authentication server to use in AKA process.

I.5.1.6 Secondary authentication protocol in 5G based on quantum security

Use case ID	UC-5-1-6
Short description	This use case describes two newly designed schemes EAP_QSSE (Quantum Secure Symmetrical Encryption) and EAP_QSSEH (Quantum Secure Symmetrical Encryption and Hash-function) based on quantum security. Both authentication parties use quantum random numbers as authentication factors, and quantum key distribution network (QKDN) to share keys, for two-way authentication of UE and AAA, to achieve lightweight and fast 5G network secondary authentication in a symmetrical encryption authentication manner.

I.5.2 QKD in SDN/NFV based network

I.5.2.1 Secure SDN and NFV Control and Management Plane

Use case ID	UC-5-2-1
Short description	The adoption of SDN and NFV technologies brings many benefits to the network, like the reduction of the complexity and costs of operating the entire infrastructure or the reduction of vendor's block-in in the systems layer (e.g., NMSs). However, the network can be affected by some threats that were not present before, as the configuration of the network elements and the images of VNFs must be transferred from central offices, network controllers and orchestration platforms. To tackle this issue, QKD can be seen as an additional security layer that runs in parallel (or also integrated) to the transport network. QKD can help to mitigate such threats, securing the communications in the control and management plane.

I.5.2.2 Quantum encryption for end-to-end services

Use case ID	UC-5-2-2
Short description	As SDN and NFV technologies are being progressively adopted in transport networks, they also open the market for new capabilities and services to be provided by the operators. SDN allows new technologies and solutions to be integrated in the network at a faster pace. One of the most demanded capabilities is an increase on the security standards of network services, as big corporations have to transfer data between their secure headquarters and data centres. These services (usually enterprise VPNs for business to business -B2B- communications) rely in underlying security protocols that are at risk of future attacks, more when speaking about data meant to have everlasting security. Also, depending on the service being deployed, the security can be implemented at different layers (e.g., IPsec, MACsec, Optical Transport Network - OTN). Quantum key distribution can be seen as a measure to provide such future-proof security, if it is appropriately used by other security systems (e.g., HSMs, VNFs, network cards, etc.) and automated via management systems. This use-case combines QKD systems to secure end-to-end (E2E) services (e.g., transport tunnels, VPNs) between remote premises. Protocols like PCEP (Patch Computation element Protocol) and MPLS (Multiprotocol Label Switching) are used and modified to use QKD.

I.5.2.3 Quantum security for service chaining

Use case ID	UC-5-2-3
Short description	The changing behaviour of current network services is forcing operators to evolve from traditional/legacy, non-scalable and rigid networks towards new flexible architectural solutions. The lead on this evolution comes from multiple sources, being Network Functions Virtualization (NFV) one of the most radical and popular trends. But the flexibility brought by these new networking trends carry associated vulnerabilities and implications. For instance, in a virtualized environment, several functions might be deployed in distributed locations for composing a service function chain (SFC). Both control and data communications must be appropriately secured, as any attempt to compromise a virtual function or its behaviour can compromise the entire infrastructure. A wide-spread concern about virtualized network elements is related to traffic attestation. Any network device deployed in a production network must be capable of assessing if a specific traffic flow passes through it and is correctly forwarded. If a node cannot guarantee this capability, it won't be accepted for production deployment. By progressively changing physical network functions (PNFs) by virtual network functions (VNFs), this task becomes harder. As the traffic traverses multiple intermediate nodes (possibly, out of the control of the VNF operator), it could eventually bypass a critical node within the SFC (e.g. a firewall). In order to mitigate this issue, a proof-of-transit technique has been developed to verify if a packet has traversed all the nodes within a path. QKD is used to provide order to the proof of transit as well as a security enhancement. Having also the continuous flow of keys provided by QKD and the speed of symmetric encryption also reduces the overhead and higher flows can be managed.

I.5.3 QKD in blockchain network

I.5.3.1 Quantum-secured blockchain

Use case ID	UC-5-3-1
Short description	It is well known that blockchain encounters severe security threat from quantum computing as its security is based on public key exchange algorithm, e.g., ECC. This use case describes a one quantum-safe blockchain solution based on QKD proposed by authors from RQC. The main idea is to replace the PoW based consensus mechanism with the Byzantine algorithm based one. For the new consensus mechanism, it does not need public key exchange for authentication, but it relies on QKD to realize information-theoretically secure authentication for pairwise nodes within the blockchain network. Due to the abandon of public key algorithm, it can be considered as quantum-safe blockchain.

I.5.3.2 Quantum vault for blockchain

Use case ID	UC-5-3-2
Short description	ID Quantique and its partners have proposed one quantum vault solution to utilize QKD and QRNG to enhance the security of blockchain. It is considered that the major pain point of blockchain technology is the secure storage of private keys. the vault is the traditional popular solution for managing blockchain private keys which is based HSM. Hereby the quantum vault solution utilizes QRNG to produce true random number as secret key seeds and uses Shamir key sharing algorithm to split the keys into multiple elements, and then use QKD to securely distribute the key elements to distributed distant key storage nodes.

I.5.4 QKD in TSN network

Use case ID	UC-5-4
Short description	The Time-sensitive Networking (TSN) is one widely applied communication standard developed by IEEE to meet the stringent latency and timing requirements of industrial environment. Ensuring cybersecurity is also an important requirement in life-critical control systems for which industrial TSN will provide communication. While private key exchange which requires manually pre-sharing keys and public key exchange which requires more computing resources are discouraged for the TSN targeted scenario, QKD can be one possible solution for TSN.

I.5.5 QKD in SCION

Use case ID	UC-5-5
Short description	Despite the fast advancement of internet-based services, the architecture and core protocol have remained mostly the same for decades since the internet's inception. However, to accommodate ever increasing and diverse data services more efficiently and securely, a new architecture is necessary, and several efforts have been made for a next-generation internet architecture. QKD can play an important role in a new internet architecture for enhancing the security which is one of the main the concern that today's internet is facing. One example use case introduced here is the QKD integration with SCION (Scalable, Control and Isolation on Next-Generation Networks) which is a research project lead by researchers at ETH Zurich. SCION aims to offer a communication infrastructure that remains highly available even in the presence of adversaries.

I.6 QKD applied in different vertical sectors

I.6.1 QKDN for smart factory

Use case ID	UC-6-1
Short description	A commercial QKD network for smart factory is being deployed in Korea. This network applied QKD to leased line between Hyundai Robotics and KT office in Daegu. Hyundai Robotics manufactures industrial robots, applies them to overseas industrial facilities, and remotely operates through various ICT infrastructure such as IoT device, leased line and servers. In this process, a malicious hacking threat on optical cable of leased line may cause production disruption due to confidential leaks. To prevent such problems, the QKD network is installed to protect corporate information and to enhance security.

I.6.2 QKDN for social safety

Use case ID	UC-6-2
Short description	A commercial QKD network for social safety is being deployed in Korea. This network applied QKD to drone communication between two adjacent local governments in Gangwon-do. Local governments operate drone-based surveillance system for public safety. In particular, since it is necessary to be careful about information leakage in areas adjacent to military camps, QKD networks are applied to drone communication. By injecting the quantum encryption key supplied from QKD into the drone, not only the drone control signal is protected, but also the video signal from the drone is encrypted and protected to improve security.

I.6.3 QKDN for medical centre

Use case ID	UC-6-3
Short description	A commercial QKD network for medical centre was deployed in Korea. This network applied QKD to leased line between St. Mary's Hospitals and their data centre in Seoul. In St. Mary's Hospital, a large medical institution, the central medical data server manages the medical data of branches located in various regions, and the branches share medical data such as patient information, medical records through the central medical data server. In this sharing process, there is a possibility that medical information, which is personally sensitive information, may be leaked by hacking. To prevent such threats, a QKD network is applied between medical data servers to encrypt medical data and improve security.

I.6.4 QKDN for secure mVoIP

Use case ID	UC-6-4
Short description	A commercial QKD network for secure mVoIP was deployed in Korea. This network applied QKD to VoIP communication between two smart phones. In mVoIP, there are threats of hacking such as voice terminal wiretapping, voice network wiretapping, and session hijacking attack. The KSA key is received from QKDN and injected into the secure communication devices. The mVoIP voice call data is encrypted through the devices.

Bibliography

[b-ETSI GR QSC 006]
TBD

_____