ITU-T Focus Groups

FG-QIT4N: Focus Group on Quantum Information Technology for Networks

Briefing session on FG-QIT4N deliverables to SG17

12 May 2022

Impacting the Information Society

- Quantum 2.0[1] is an emerging nascent technology area that is likely to have a significant global impact on ICT network architectures of the future
  - **Conventional Information Technology:** Quantum mechanics plays a "*supporting role*" (e.g., materials, devices, etc.)
  - **Quantum Information Technology (QIT):** Fundamental quantum phenomena play "*center stage*" to applications in Quantum Information Processing and Communication (QIPC)[2] as well as security
- QIT includes
  - Quantum computing
  - Quantum Key Distribution (QKD) and Quantum Teleportation
  - Quantum sensing, random number generation (QRNG), and etc.
- While still in its infancy, QIT standardization activities are taking root (ITU-T, ETSI, ISO/IEC, IEEE)
- Significant investments are being made by the international community
- It is important now to consider and *carefully* prepare for the rapidly changing landscape of ICT networks to ensure seamless interoperability and ubiquitous access to information, as well as to promote a competitive and proliferated marketplace

[1]J P Dowling and G J Milburn, "Quantum technology: the second quantum revolution," *Philos. T. Roy. Soc. A* **361** (2003)

[2]T P Spiller and W J Munro, "Towards a quantum information technology industry," *J. Phys.: Condens. Matter* **18** (2006)

Terms of Reference - Objectives

- **Considering evolution and applications of QIT for networks,**
- The topics of study include:
  - **Telecom/network aspects of QKD networks** that are identified in close coordination with ITU-T SG13 and SG17 as not within the scope of SG13 (QKD network architecture aspects) and SG17 (security aspects of QKD networks and applications of QRNG for security)
  - **QIN technology and network evolution**
- **The FG outputs will focus on terminology and use cases.** The FG will reference relevant terminology defined in the pertinent ITU-T SGs. When necessary, the FG will liaise with the relevant SGs if terminology needs to evolve to take into account technology evolution.
- **To provide necessary technical background information and collaborative conditions** in order to effectively support QIN-related standardization work in ITU-T study groups.
- **To provide an open cooperation platform with ITU-T study groups and other SDOs,** including collaborative standardization work, co-located meetings, and workshops on quantum topics.

https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/ToR.aspx

FG-QIT4N Working Structure

Co-Chairmen

- Mr. Alexey Borodin, Rostelecom, Russian Federation
- Mr. James Nagel, L3Harris Technologies, USA
- Mr. Qiang Zhang, University of Science and Technology of China (USTC), China

Working Group Chairs

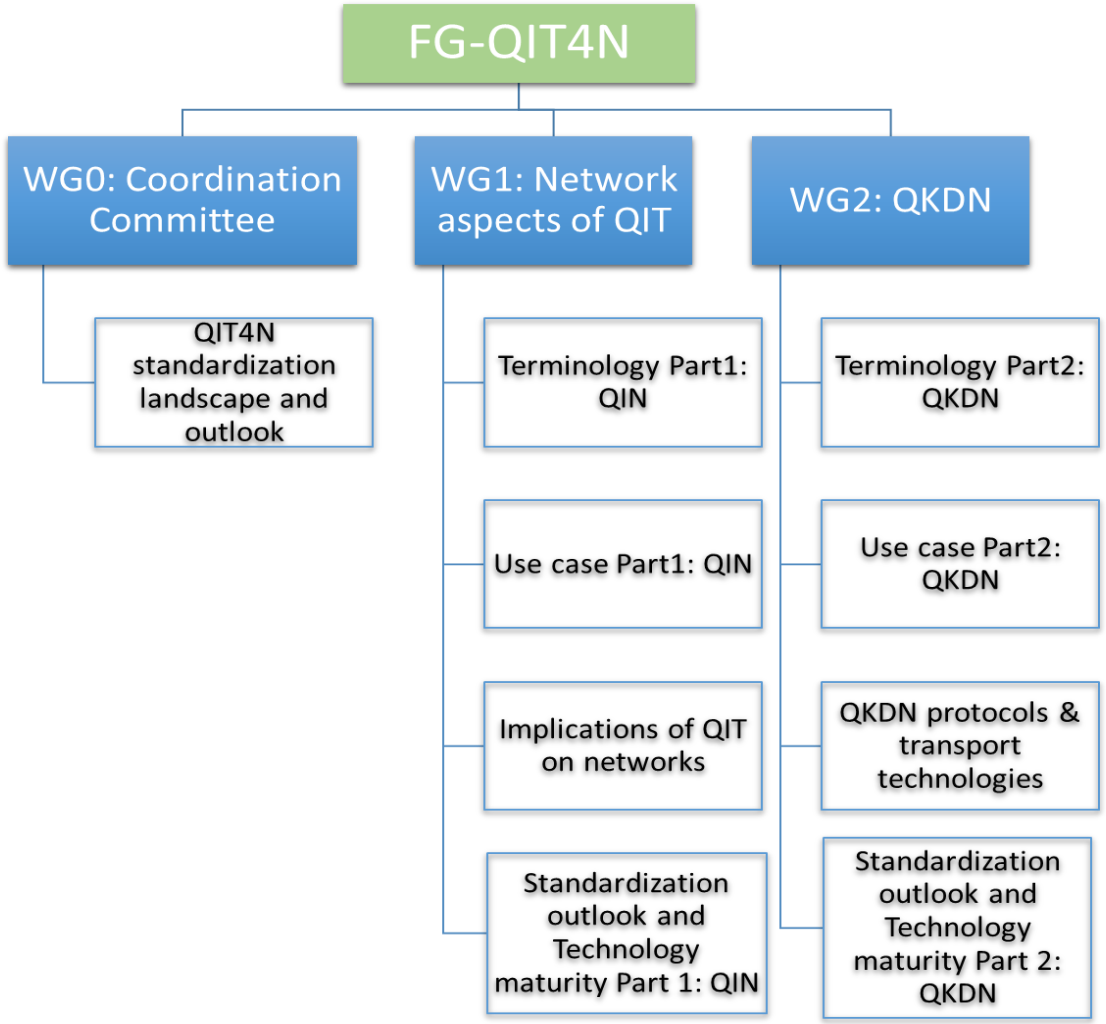
- WG0: Co-Chairmen
- WG1: Mr. Helmut Griesser, Adva Optical Networking, Germany
- WG2: Mr. Zhangchao Ma, CAS Quantum Network, China

WG1: Network aspects of QIT

To provide technical context in relation to the study topics and deliverables related to network aspects of quantum information technology

WG2: QKDN

To provide technical context in relation to the study topics and deliverables related to quantum key distribution networks and those aspects not covered in SG 13 and SG 17



FG-QIT4N Activities

Activities throughout the lifetime of the Focus Group have included…

- **Collaboration and cooperation with ITU-T study groups and other SDOs and sub-groups**
  - Formal liaisons
  - Joint meetings with ETSI (ISG QKD) and ISO/IEC (JTC 1 SC27/WG3)
  - Informational presentations by industry and academia groups at plenary meetings
- **Development and writing of technical reports**
  - Evolution and applications of QIT for networks
  - Evolution of Quantum Information Networks (QIN), focused on terminologies and use cases
  - Telecom/network aspects of QKD networks that are not currently within the scope of SG13 and SG17, focused on terminologies, new use cases, protocols and transport technologies
- **Organizing and hosting of the FG-QIT4N QIT Webinar series***
  - *Cybersecurity in the Quantum Era* (WSIS Forum 2021 – w/ ETSI ISG QKD)
  - *Joint Symposium on Quantum Transport Technology* (w/ IEEE and IEC)
  - *Quantum Information Technologies (QIT) for Networks – Use Cases*
  - *Harmonisation of Terminology in Standards for Quantum Technology* (participation of ITU, ISO, IEC, and ETSI)
  - *Joint Symposium on Quantum Photonic Integrated Circuits* (w/ IEEE and IEC)

*All webinars recorded and available for viewing at https://www.itu.int/en/ITU-T/webinars/qit/Pages/default.aspx

Presentation of Deliverables

- **Standardization outlook and technology maturity:**
  - *Quantum key distribution networks,* **Junsen Lai**, CAICT, China | FG QIT4N D2.5 Chief Editor
  - *Network aspects of quantum information technologies*, **Barbara Goldstein**, NIST, United States | FG QIT4N D1.4 Chief Editor
- **Terminology:**
  - *Quantum key distribution networks,* **K Karunaratne**, Qubitekk, United States | FG QIT4N D2.1 Chief Editor
  - *Network aspects of quantum information technologies*, **Ming-Han Li**, CAS Quantum Network, China | FG QIT4N D1.1 Chief Editor
- **Use cases:**
  - *Quantum key distribution networks,* **Zhangchao Ma**, CAS Quantum Network, China | FG QIT4N D2.2 Chief Editor
  - *Network aspects of quantum information technologies*, **Yuan Gu**, ZTE Corporation, China | FG QIT4N D1.2 Chief Editor
- **Quantum key distribution network protocols:**
  - *QKDN protocols: Quantum layer,* **Hao Qin**, NUS, Singapore | FG QIT4N D2.3 Part 1 Chief Editor
  - *QKDN protocols: Key management layer, QKDN control layer and QKDN management layer*, **Hongyu Wu**, QuantumCTek Co., Ltd. China | FG QIT4N D2.3 Part 2 Chief Editor

*All deliverables are available for free download at: http://www.itu.int/go/fgqit4n

Relevance of D2.5 to SG17

- **Title:** Quantum information technology for networks **standardization outlook** and **technology maturity**: Quantum key distribution network
- **Scope and summary:**
  1. Quantum key distribution (QKD) technology, including **frontier research, system experiment, field trial,** and **commercialized product**.
  2. QKD industry status, including **market players** such as system vendor, network provider, **projects** and **opinions** from different countries and areas.
  3. QKD network **standardization landscape**, conducts **gap analysis**, and provides future standardization **suggestions**.
- **QKD technology and application information,** such as research and experiment progress, commercialization product and market player status, various project and opinion from different countries and stake-holders, are provided for technology maturity reference. **QKD standardization** progress of international SDOs and future requirement are solicited and analyzed.
- **Main target of QKD application** is to improve the security of symmetric encryption. For the network security topic and standard in SG17, information such as QKD technology maturity, commercialization status, and deployment progress can be **considered for future standardization**.

Relevance of D1.4 to SG17

Standardization Readiness *update*

Post-Quantum Cryptography *update*

2016 Criteria and requirements and call for proposals

2017 Received 82 submissions and announced 69 1st round candidates

2018 The 1st NIST PQC standardization Conference

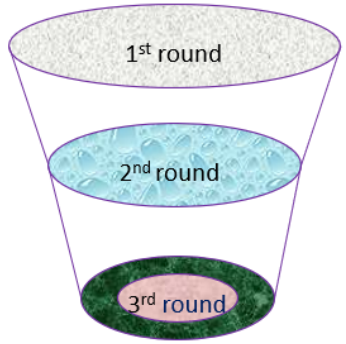
2019
Announced 26 2nd round candidates

The 2nd NIST PQC Standardization Conference

2020 Announced 3rd round 7 finalists and 8 alternate candidate

2021
The 3rd NIST PQC Standardization Conference

2022-2023 Release draft standards and call for public comments



NIST will announce the selection very soon!

Lily.chen@nist.gov

QKD	PQC
Doesn't rely on computing complexity assumptions	Relies on computing complexity assumptions
Uses quantum mechanics to distribute keys	Doesn't rely on quantum mechanics; drop-in replacement
May be used to establish keys. Relies on PQC for authentication. Cannot provide signature function.	Can create signatures & fit into existing infrastructure for certificate validation. Signature function can be used for code-signing to protect against malware/malicious software

QKD can be used with PQ authentication (KEM) for additional security.

Briefing on FG-QIT4N D2.1

- **Title:** **Quantum information technology for networks terminology: Quantum key distribution network**
- **Summary:** This technical report is a deliverable of the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N). This technical report provides a survey of terminology relevant to QKDN currently published or under development by SDOs including ETSI ISG QKD, ISO/IEC JTC1 SC27 WG3 and ITU-T SG13/17. Based on the survey, the terms are categorized according to the specific technical directions they fall under.
- **Scope :** This Technical Report contains a set of definitions of terms commonly used in quantum key distribution networks (QKDN). The terminologies have been obtained from work done by Standards Development Organizations (SDOs) and are categorized according to the specific technical directions they fall under.
- **Editor team:**

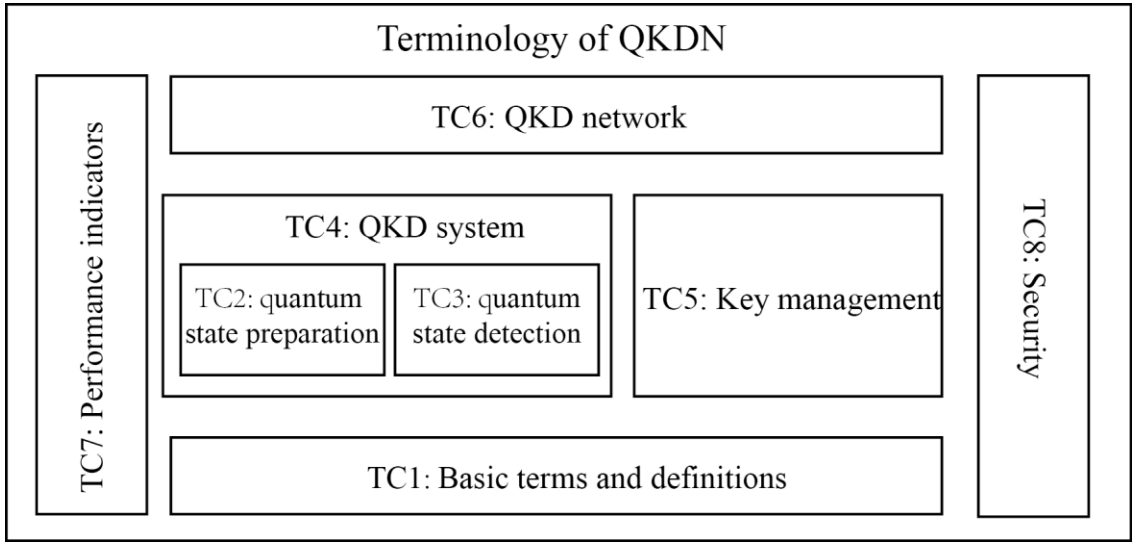
- **Chief editor**: K. Karunaratne **Email**: kkarunaratne@qubitekk.com
- **Co-editor :** Yan Jiang **Email**: yan.jiang@quantum-info.com

- **Direct link to D2.1 report:** https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-QIT4N-2021-D2.1-PDF-E.pdf

Briefing on FG-QIT4N D2.1

- **QKDN relevant terminologies collected from the following sources:**
  - **ETSI ISG QKD:** GR QKD 007 Quantum Key Distribution (QKD); Vocabulary (published in 2018) **and its latest drafting updates (v1.3.2)**
  - **ISO/IEC JTC1 SC27 WG3:** ISO/ IEC 23837 Security requirements, test and evaluation methods for quantum key distribution (still in the drafting stage CD2)
  - **ITU-T SG13/17:** published Recommendations on QKDN, i.e., Y.3800, Y.3802, Y.3803, Y.3806, X.1702, X.1710

- **Result of this survey:**
  - **Collect 172 terms relevant to QKD/QKDN**
  - **The terms are categorized into 8 classes**



Relevance of D1.1 to SG17

- Terminology related to QRNG
  - Can be used for further development in SG17
  - **X.1702** Quantum noise random number generator architecture
  - Other required terms in the future work (like DI, Semi-DI, etc.)
  - Need to review D1.1 for the harmonization of terminologies
- Terminology related to QITs
  - Can be used for further development in SG17
    - Quantum time synchronization
    - Quantum cloud computing

Briefing on FG-QIT4N D2.2

- **Title:** **Quantum information technology for networks use cases: Quantum key distribution network**
- **Summary:** It consolidates the QKDN use cases gathered during the lifetime of the ITU-T FG QIT4N. The QKDN uses cases are classified into 6 classes and the report highlights the competitive advantage of the use cases brought by QKDN and provides suggestions for future standardization efforts.
- **Scope:**
  - Competitive advantages brought by QKDN
  - Overview of QKDN use cases
  - Collected QKDN use cases categorized into 6 classes
  - Suggestions for future work
- **Editor team:**

Zhangchao MA, CAS Quantum Network Co., Ltd., China	Email: mazhangchao@qtict.com
Terrill FRANTZ, Harrisburg University of Science and Technology, United States	Email: terrill@org-sim.com
Thomas LAENGER, Austrian Institute of Technology (AIT), Austria	Email: thomas.laenger@gmx.at
Dong-Hi SIM, SK Telecom, Korea, Republic of	Email: donghee.shim@sk.com
Andreas POPPE, Austrian Institute of Technology (AIT), Austria	Email: Andreas.Poppe@ait.ac.at

- **Direct link to D2.2 report:** https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-QIT4N-2021-D2.2-PDF-E.pdf

Competitive advantages of using QKDN

Quantum computing resistance

- Compared with conventional computation-complexity-based cryptography, QKD can be considered as one of the means to combat quantum computing threats

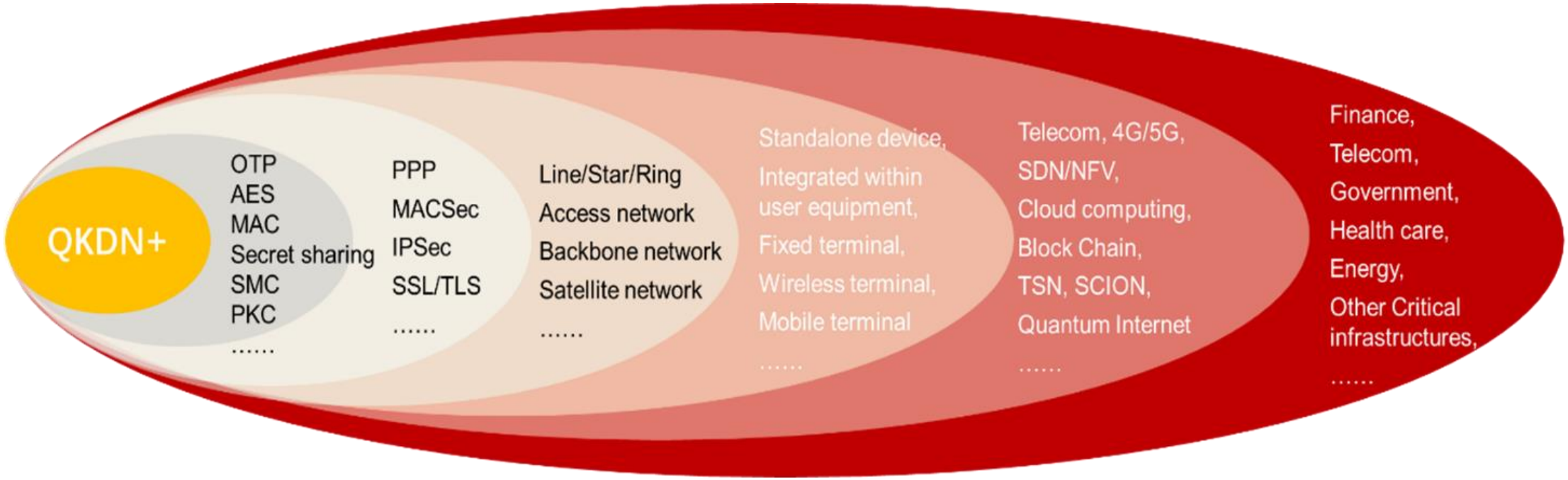
Perfect forward security (PFS)

- Compared to conventional symmetric cryptography, QKD systems can guarantee PFS since the keys are continuously refreshed and can thus only be used once.

High performance key generation

- 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.

QKDN use cases classified into 6 classes



QKD + | Cryptography | TCP/IP protocols | Topology | Terminal types | Network forms | Vertical sectors

Relevance of D1.2 to SG17

- QRNG
  - DIQRNG, Semi-DIQRNG, device-dependent QRNG
    - Security (High --> Low) / Practicality (Low --> High)
  - Can be used as input for
    - Possible enhancement to the existing QRNG related work in SG17 (like Rec. X.1702 QRNG Arch)
    - Other possible standards work in the future required for network aspect of QRNG

- Quantum communication tasks concerning security
  - Quantum digital signatures, quantum anonymous transmission, quantum money
    - Enabling technologies still at very low readiness level: quantum repeaters, quantum memories, quantum entanglement distribution devices
    - The stages of development of quantum communication networks required to deploy those use cases stand in between the current stage (QKD networks) and a large-scale quantum internet that would connect quantum computers with quantum communication channels
  - Can be used as input for the future work on requirements and relevant framework of quantum communication beyond QKD in SG17 (X.1700 series)

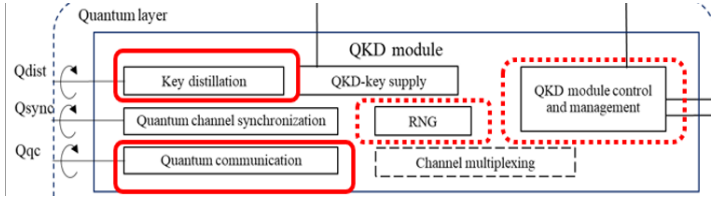
Relevance of D2.3 part 1 to SG17

- **Scope & Summary:**

❑ Study and review protocols in the quantum layer of QKDN

❑ Focuses on QKD protocols, the core technology in QKDN:

- General aspects: Workflow; Categories
- Security: Security notions, Epsilon security, Implementation security
- Introduction of discrete variable (DV) QKD protocols
- Introduction of continuous variable (CV) QKD protocols
- Standardization analysis and suggestions



- **Editing team:**

❑Chief editor: **Hao Qin**, National Quantum-Safe Network|National University of Singapore, Email: hao.qin@nus.edu.sg

❑Co-editors: **Peng Huang**, Shanghai Jiao Tong University, XT Quantech, Email: huang.peng@sjtu.edu.cn

Hongyu Wu, QuantumCTek, Email: hongyu.wu@quantum-info.com

Relations to SG17

❑ **Quantum layer standardization is missing**

- QKD is the core part of quantum layer and QKDN
- QKD protocol is relatively a **new** concept to SDOs
- QKD protocol owns the features of both cryptographic protocols and communication protocol
- **Security** is the core of QKD protocol

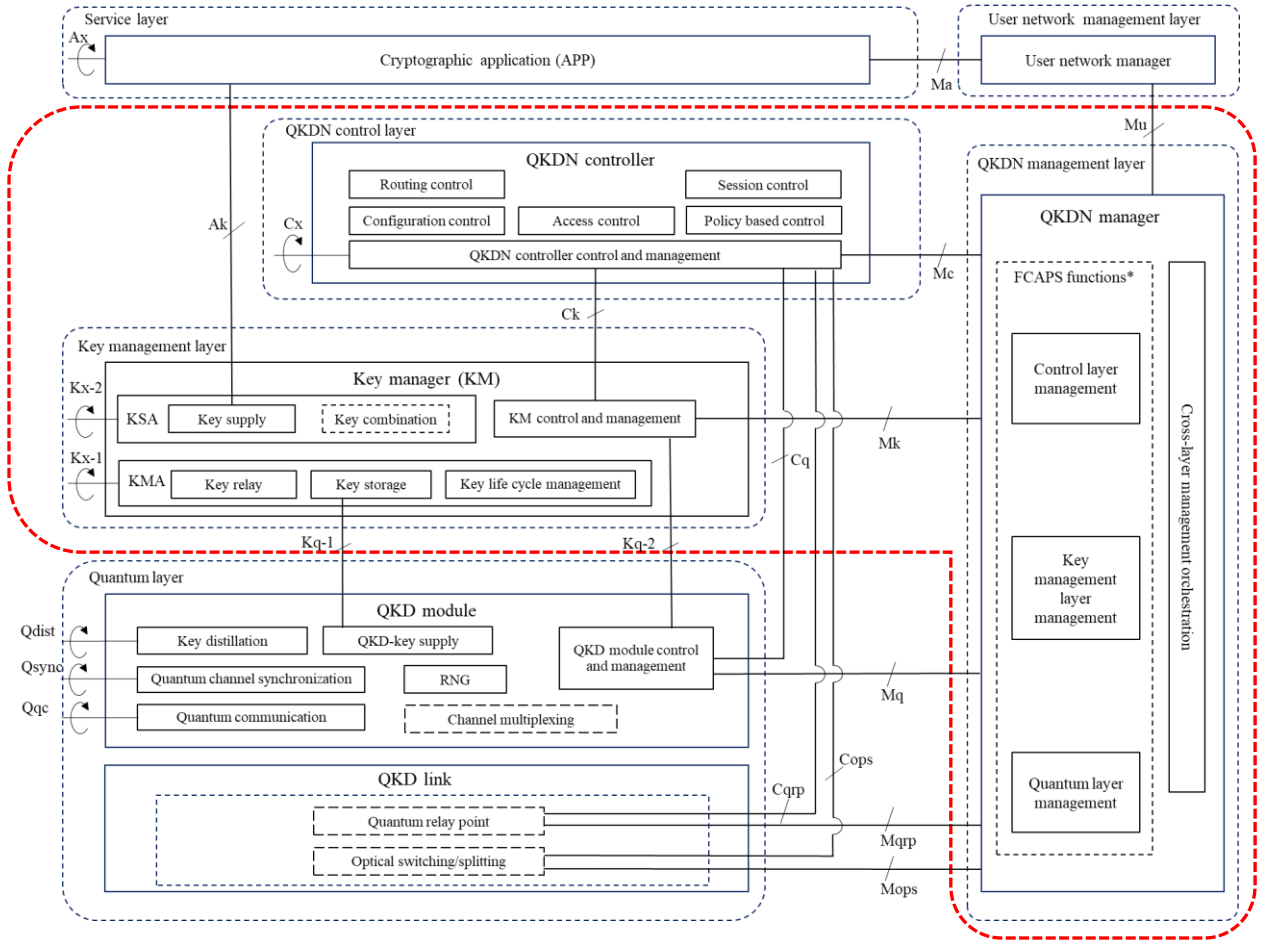
❑ **QKD protocol framework**

- Many QKD protocols in academic and industry
- Protocol **workflow & pattern** serves as basis of the framework
- Each step in a QKD protocol is **security concerned**
- Needed to further define **specific** QKD protocols

❑ **Various security topics on QKD protocol**

- **Unique security** features of QKD protocol
- Information-theoretic security (**ITS**) and beyond
- **Security** notions, epsilon **security** and finite size
- Theoretical **security** and implementation **security**
- Security requirements and measures

Relevance of D2.3 part 2 to SG17



A functional architecture model of QKDN

Each reference point represents an interface with underlying protocol to be developed.

SG11

There is a specific clause on "Security considerations" in each work item of protocols for Ak, Kx, Ck and Kq-1 interfaces.

SG17

QKDN is intrinsically related to security issues.

For more information:

Contact:

- The WG chairs and editors via email addresses in the slides, or
- Secretariat at: **tsbfgqit4n@itu.int**

Visit the website:

http://www.itu.int/go/fgqit4n

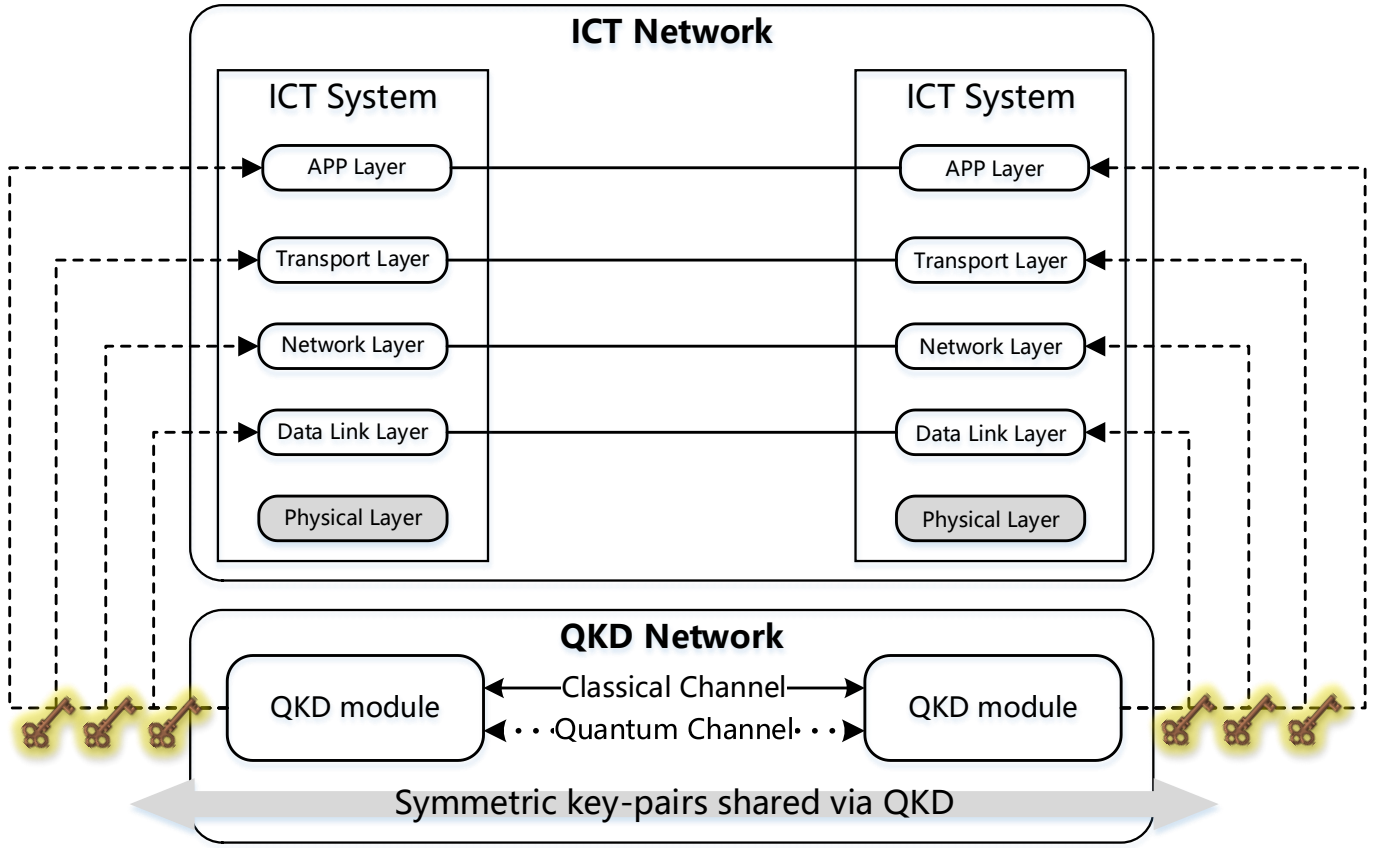
Supplementary slides for D2.2

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 **(detailed in UC-1-1);**
- **Secure multi-party computation (SMC):** QKD raw key can be used to implement oblivious key transfer to perform SMC **(detailed in UC-1-2);**;
- **Public key cryptography (PKC):** QKD can be combined with PKC including PQC to provide hybrid security guarantee **(detailed in UC-1-3);**.

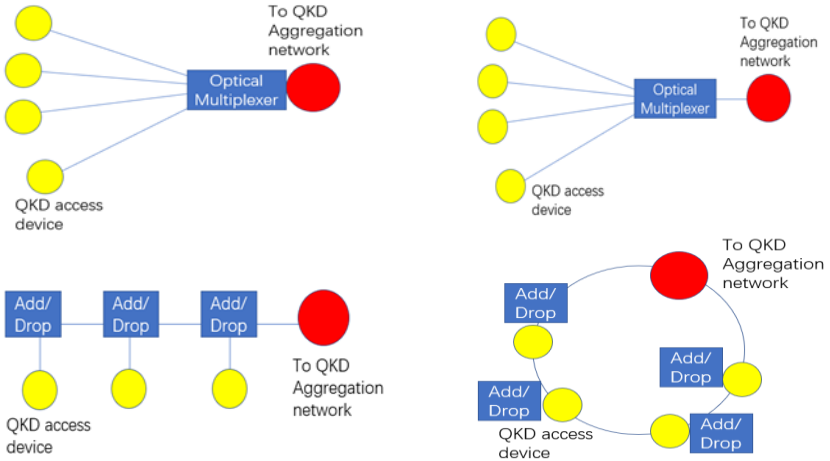
UC2: QKD integrated with various TCP/IP protocols

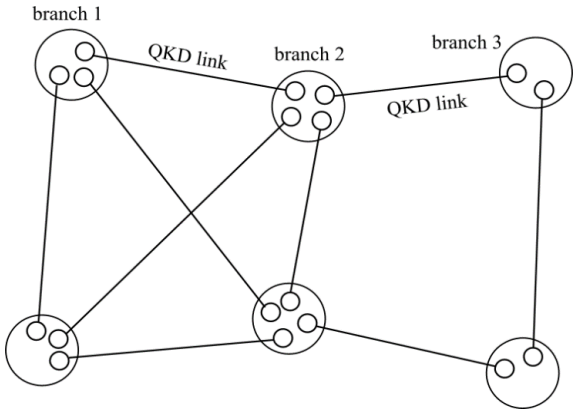
- **QKD can be integrated with TCP/IP protocols at various layers, e.g.,**
  - PPP and MACSec protocol at MAC layer **(detailed in UC-2-1);**
  - IPSec protocol at network layer **(detailed in UC-2-2);**
  - TLS protocol at transport layer **(detailed in UC-2-3);**
  - User defined protocols at application layer **(detailed in UC-2-4);**

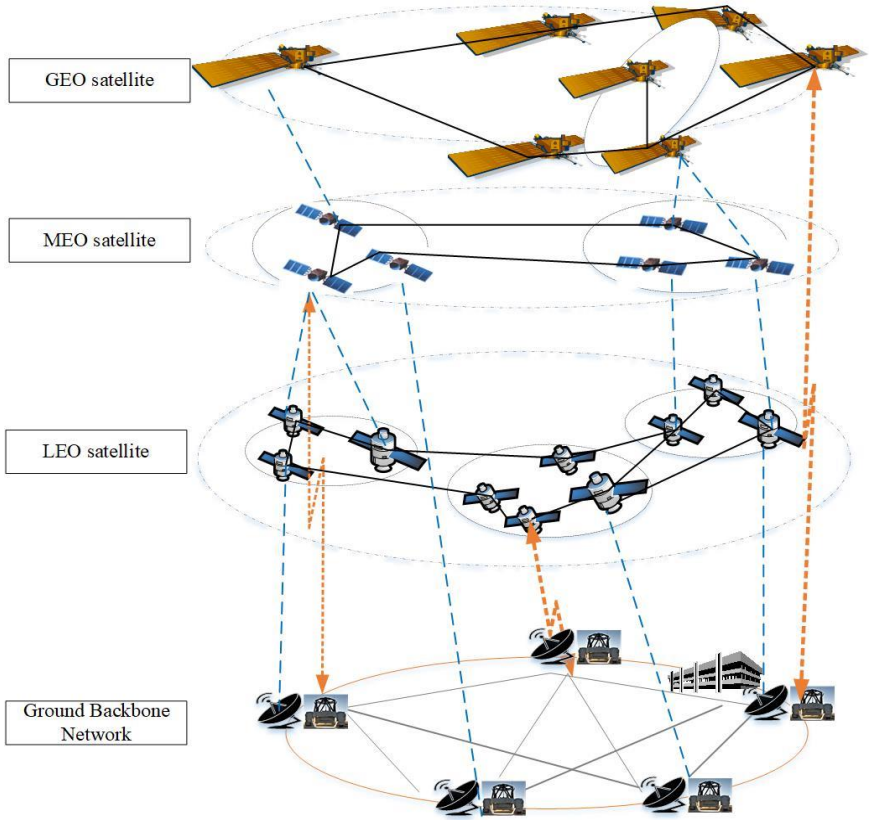


UC3: QKD deployed in various network topologies

- **QKD can be implemented in various network topologies e.g.,**
  - line or ring or star topology
  - fibre-based metropolitan access network **(detailed in UC-3-1);**
  - fibre-based inter-city backbone network **(detailed in UC-3-2);**
  - free-space satellite-ground or inter-satellite network **(detailed in UC-3-3);**

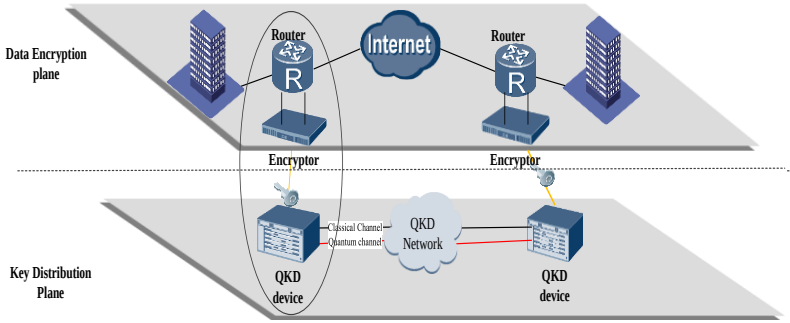


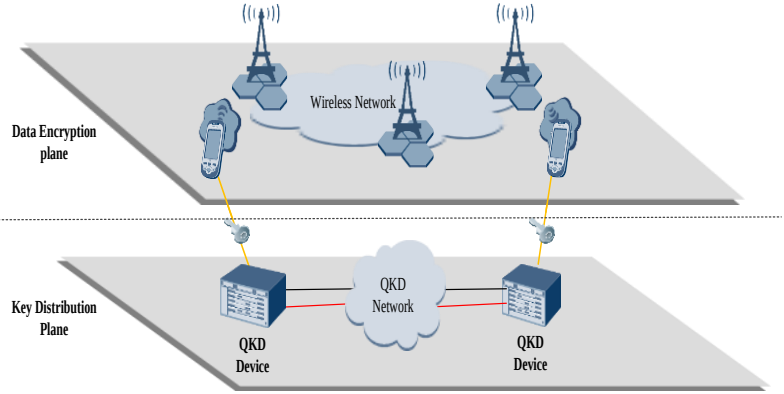


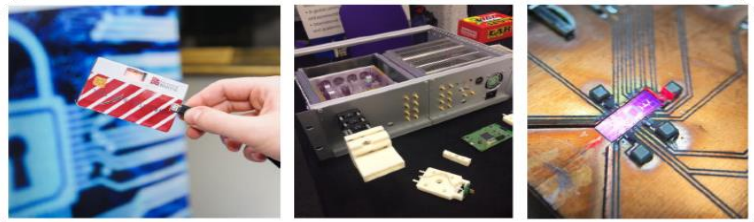


UC4: QKD with different user device categories

- **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 **(detailed in UC-4-1);**
  - Wireless user device which integrates QKD module to consume online keys provided by QKDN **(detailed in UC-4-2);**.





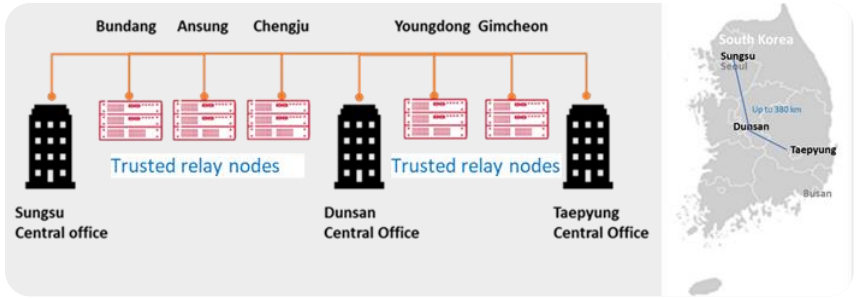


Sibson, P., et al. (2017). "Networked Quantum-Secured Communications with Hand-held and Integrated Devices: Bristol's Activities in the UK Quantum Communications Hub. " QCrypt 2017.

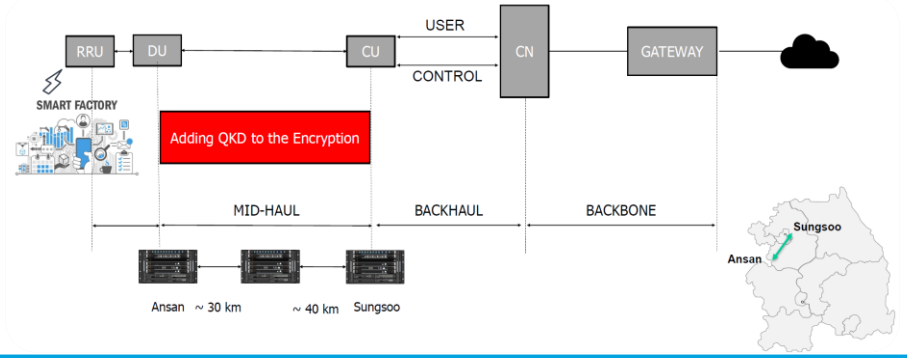
UC5: QKD integrated in various network forms

- **QKD can be integrated in various ICT network forms which require high security guarantee, e.g.**
  - 4G/5G network (detailed in UC-5-1),
  - SDN/NFV based network (detailed in UC-5-2),
  - Block chain network (detailed in UC-5-3)
  - TSN network (detailed in UC-5-4)
  - SCION (detailed in UC-5-6),
  - quantum internet

QKD for LTE backhaul in Korea



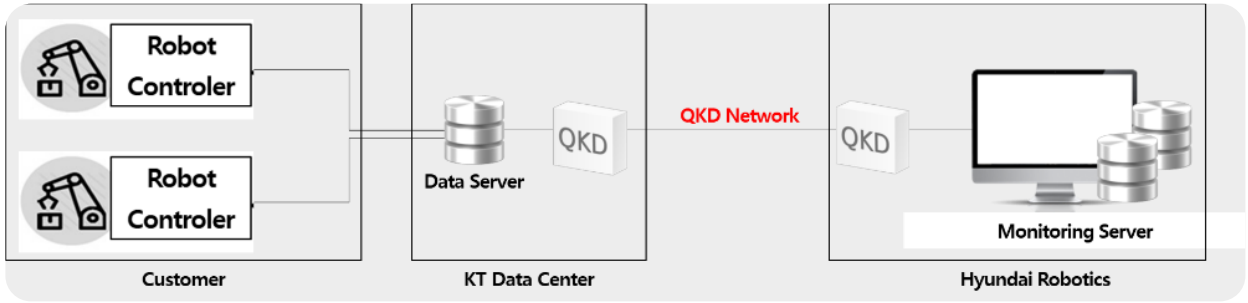
5G mid-haul QKD in Korea



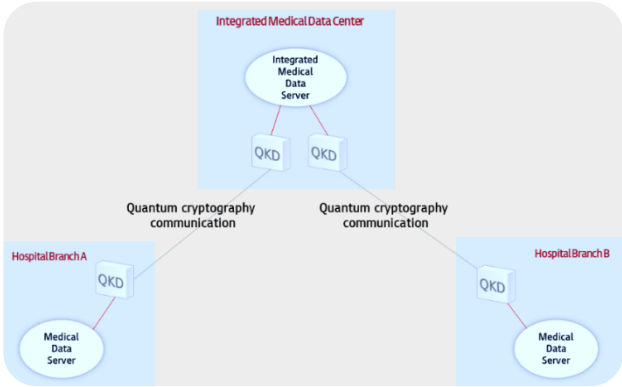
UCC6: QKD applied in different vertical sectors

- QKD can be applied in various vertical sectors which require high level and long-term security, e.g., Finance, Government, Health care, public safety, Telecom industry, energy, transportation

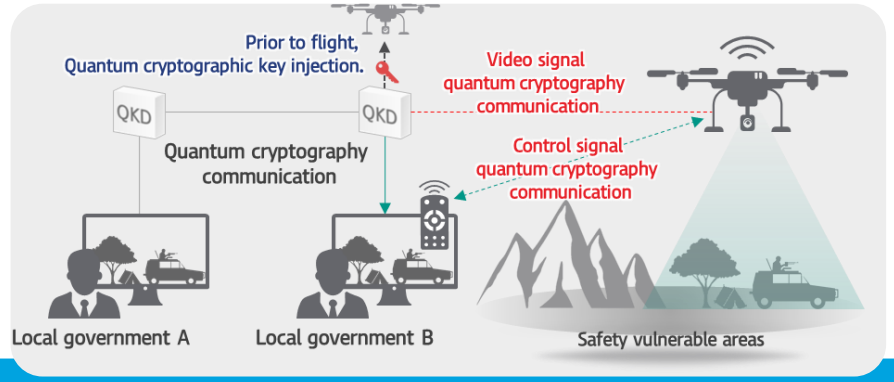
QKDN for smart factory



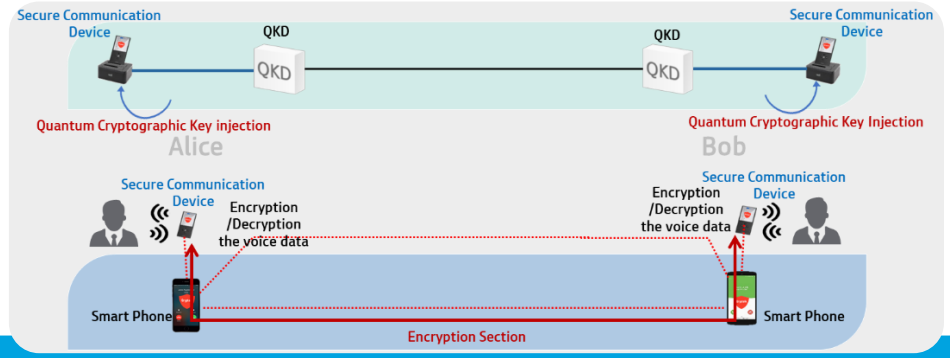
QKDN for medical centre



QKDN for Social safety



QKDN for secure mVoIP



UCC1: QKD combined with other cryptographic primitives

Use case ID	UC-1-1 QKD combined with secret sharing
Contributor	Thomas Länger; Austrian Institute of Technology (AIT)
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.

UCC1: QKD combined with other cryptographic primitives

Use case ID	UC-1-2 QKD combined with SMC
Contributors	Armando Pinto; University of Aveiro Vicente Martín; UPM – Universidad Politécnica de Madrid
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.
References	[b-Lemus] and [b-Pinto]

UCC1: QKD combined with other cryptographic primitives

Use case ID	UC-1-3 Hybrid QKD and PQC for encrypted communications
Contributors	Zhangchao Ma; *CAS Quantum Network Co., Ltd.*
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.
References	[b-Leilei]

UCC2: QKD integrated with various TCP/IP protocols

Use case ID	UC-2-1 QKD integrated in data link layer
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.
References	Section 6.2 of [b-ETSI GS QKD 002]

Use case ID	UC-2-2 QKD integrated in network layer
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.
References	Section 6.2 of [b-ETSI GS QKD 002]

UCC2: QKD integrated with various TCP/IP protocols

Use case ID	UC-2-3 QKD integrated in transport layer
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.
References	Section 6.3 of [b-ETSI GS QKD 002]

Use case ID	UC-2-4 QKD integrated in application layer
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.
References	Section 6.4 of [b-ETSI GS QKD 002]

UCC3: QKD implemented in various network topologies

Use case ID	UC-3-1 QKDN as metropolitan access network
Contributor	Thomas Länger; Austrian Institute of Technology (AIT)
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.

Use case ID	UC-3-2 QKDN as inter-city backbone network
Contributor	CAS Quantum Network Co., Ltd.
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.
References	[b-Zhang-1] and [b-Zhang-2]

UCC4: QKD with different user device categories

Use case ID	UC-4-1 Wireless user device with offline QKD-keys
Contributors	Zhangchao Ma; CAS Quantum Network Co., Ltd.
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.

Use case ID	UC-4-2 Wireless user device with integrated QKD module
Contributors	Zhangchao Ma; CAS Quantum Network Co., Ltd.
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.
References	[b-Sibson]

UCC5: QKD integrated in various network forms

UC-5-1 QKD in 4G/5G networks

Use case ID	UC-5-1-1 QKDN for LTE backhaul and 5G backbone
Contributors	Mingeun Yoon and Dong-Hi Sim; SK Telecom
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.
References	[b-XSTR-SEC-QKD]

Use case ID	UC-5-1-2 Quantum secured inter-domain 5G service orchestrator
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.
References	[b-Wang-2]

UCC5: QKD integrated in various network forms

UC-5-1 QKD in 4G/5G networks

Use case ID	UC-5-1-3 QKDN for 5G front-haul
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.
References	[b-Priem]

Use case ID	UC-5-1-4 QKDN for 5G mid-haul
Contributors	Mingeun Yoon and Dong-Hi Sim; SK Telecom
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.
References	[b-Priem]

UCC5: QKD integrated in various network forms

UC-5-1 QKD in 4G/5G networks

Use case ID	UC-5-1-5 Quantum security enhancement for universal AKA authentication protocol
Contributors	Chunli Ma, Yong Zhao and Hongyu Wu; QuantumCTek Co., Ltd.
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.
References	[b-RFC4187] and [b-RFC5448]

Use case ID	UC-5-1-6 Secondary authentication protocol in 5G based on quantum security
Contributors	Chunli Ma, Yong Zhao and Hongyu Wu; QuantumCTek Co., Ltd.
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.
References	[b-3GPP TS 33.501] and [b-RFC3748]

UCC5: QKD integrated in various network forms

UC-5-2 QKD in SDN/NFV based network

Use case ID	UC-5-2-1 Secure SDN and NFV Control and Management Plane
Contributors	Vicente Martín; UPM – Universidad Politécnica de Madrid
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.
References	[b-Aguado-1]

UCC5: QKD integrated in various network forms

UC-5-2 QKD in SDN/NFV based network

Use case ID	UC-5-2-2 Quantum encryption for end-to-end services
Contributors	Vicente Martín; UPM – Universidad Politécnica de Madrid
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.
References	[b-Aguado-2]

UCC5: QKD integrated in various network forms

UC-5-2 QKD in SDN/NFV based network

Use case ID	UC-5-2-3 Quantum security for service chaining
Contributors	Vicente Martín; UPM – Universidad Politécnica de Madrid
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.
References	[b-Aguado-3]

UCC5: QKD integrated in various network forms

UC-5-3 QKD in blockchain network

Use case ID	UC-5-3-1 Quantum-secured blockchain
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.
References	[b-Kiktenko]

UCC5: QKD integrated in various network forms

UC-5-3 QKD in blockchain network

Use case ID	UC-5-3-2 Quantum vault for blockchain
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.
References	[b-Huttner]

UCC5: QKD integrated in various network forms

Use case ID	UC-5-4 QKD in TSN network
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.
References	[b-Avnu]

UCC5: QKD integrated in various network forms

Use case ID	UC-5-5 QKD in SCION
Contributors	Mingeun Yoon and Dong-hi Sim; SK Telecom Jonghoon Kwon; ETH Zürich
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.
References	[b-ETSI GS NGP 001] and [b-ETSI GS NGP 005]

UCC6 QKD applied in different vertical sectors

Use case ID	UC-6-1 QKDN for smart factory
Contributors	Miryeong Park, Chun Seok Yoon and Hyungsoo Kim; KT Corp.
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.

UCC6 QKD applied in different vertical sectors

Use case ID	UC-6-2 QKDN for social safety
Contributors	Miryeong Park, Chun Seok Yoon and Hyungsoo Kim; KT Corp.
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.

UCC6 QKD applied in different vertical sectors

Use case ID	UC-6-3 QKDN for medical centre
Contributors	Miryeong Park, Chun Seok Yoon and Hyungsoo Kim; KT Corp.
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.

Use case ID	UC-6-4 QKDN for secure mVoIP
Contributors	Miryeong Park, Chun Seok Yoon and Hyungsoo Kim; KT Corp.
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.