Preliminary Study of Advanced Technologies towards 6G Era: QITs

2021

未来移动通信论坛
FuTURE MOBILE COMMUNICATION FORUM

Preliminary Study of Advanced Technologies towards 6G Era: QITs

2021

Executive Summary

With the large-scale commercialization of 5G in 2021, the global industry has witnessed a starting of exploration and research on the 6th generation (6G) communication systems. 6G will build a new type of network that is intelligently and efficiently interconnected between humans, machine and things. On the basis of greatly improving the network capability, it has new functions such as endogenous intelligence, multi-dimensional perception, digital twin, endogenous network security and so on. With the in-depth research on 6G network and key technologies, its integration and application with Quantum Information Technologies (QITs) will become the focus in the future.

In 6G era, the importance of cybersecurity in mobile communications is expected to rise exponentially. Quantum cryptography has emerged as a potential solution for safeguarding critical information because it is impossible to copy data encoded in a quantum state. In the first part, this white paper gives an overview of Quantum Secure Communication. Starting with enabling technologies of quantum key distribution (QKD), standardization activities for QKD and its networking technologies are presented, followed by implications of QKD for 6G. In particular, two typical applications scenarios are introduced. One is the quantum encryption system that will be applied to the construction of Winter Olympics Smart Park and Xiong'an New Area. The other is in Xiong’an quantum communication pilot, where a quantum communication trunk line between Beijing and Xiong’an will be deployed, and a quantum key distribution platform will be introduced to provide security keys for customers in the fields of Internet of things, Internet of vehicles, smart energy, smart government and so on.

The provisions of a many-fold increase in the 6G communication system performance alongside with rich diversity of innovative services call for a revolutionary promotion in information processing capability. In this regard, the emerging Quantum Machine Learning (QML) has attracted significant attention due to its information processing paradigm by combining the established benefits of quantum mechanism and machine learning. In the second part, followed by preliminary knowledges of machine learning (ML) basic paradigms and their application in solving problem across different layers of in communication systems, and quantum tools, this white paper presents examples to get insight into the research of QML.

Table of Contents

1 Introduction

The scope of this annually revised white paper is to introduce quantum information technologies (QITs) with the aim of taking advantages of their powerful information processing capabilities to fulfil stringent demands of communication and computing envisaged by 6G systems. Our previous version in 2020 present the overview of QITs from the perspectives of QITs & Quantum Internet and QTIs for Classical Signal Processing, respectively. The version of 2021 will further introduce from two benefits expected from QITs to communication systems, i.e., secure communication and enhanced information processing capability.

Chapter 2. Quantum Secure Communication

In 6G era, the importance of cybersecurity in mobile communications is expected to rise exponentially. Quantum cryptography has emerged as a potential solution for safeguarding critical information because it is impossible to copy data encoded in a quantum state. Chapter 2 gives an overview of Quantum Secure Communication. Starting with enabling technologies of quantum key distribution (QKD), standardization activities for QKD and its networking technologies are presented, followed by implications of QKD for 6G. In particular, two typical applications scenarios are introduced as deploying quantum encryption system and deploying quantum communication trunk line in providing security keys for customers in the fields of Internet of things, Internet of vehicles, smart energy, smart government and so on.

Chapter 3. Quantum Machine Learning (QML)

The provisions of a many-fold increase in the 6G communication system performance alongside with rich diversity of innovative services call for a revolutionary promotion in information processing capability. In this regard, the emerging QML has attracted significant attention due to its information processing paradigm by combining the established benefits of quantum mechanism and machine learning. Chapter 3 starts with the concepts of QML on a high level and then discusses machine learning (ML) basic paradigms and their application in solving problem across different layers of in communication systems. Followed by preliminary knowledges of quantum tools, Chapter 3 presents examples to get insight into the research of QML. Consequently, QML for communication systems can be obtained by ML for communication system being synergy with quantum speedup.

2 Quantum Secure Communication

2.1 Enabling Technologies for Quantum Secure Communication

2.1.1 Overall Picture

Quantum secure communication means combing the secret key generated from quantum key distribution (QKD) device with existing symmetric encryptor. The distribution process of the secret key is guaranteed by law of quantum mechanics.

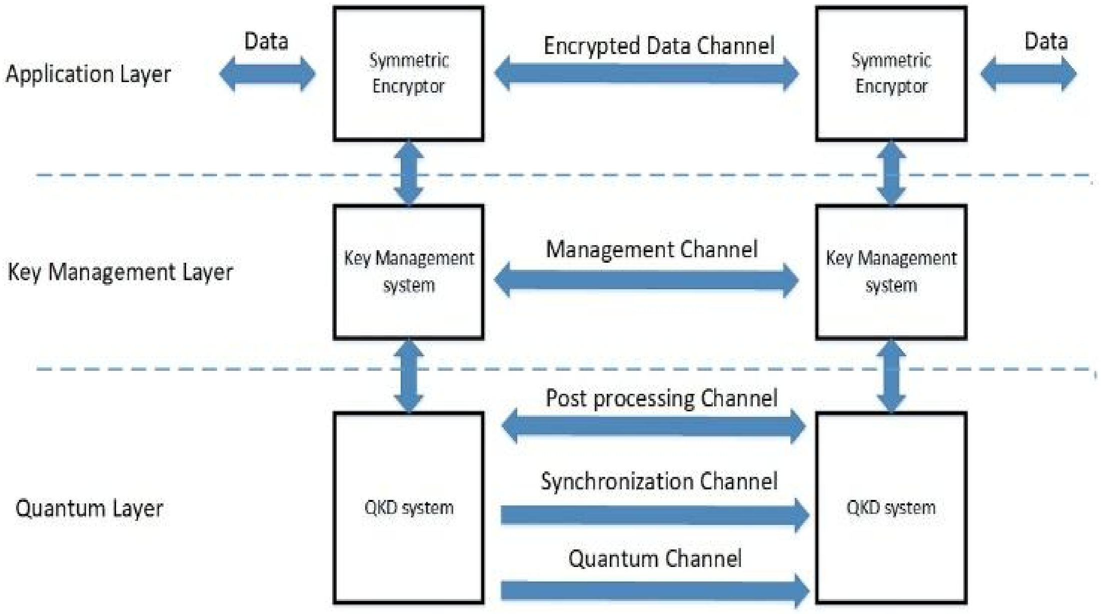


Figure 2.1 Quantum secure communication, a system view

2.1.2 Types of QKD

The types of QKD can be categorized by the behavior of transmitter and receiver, also the usage of physical degree of freedom. Based on the behavior of transmitter and receiver, the QKD types are prepare-and-measure, two transmitters to one common receiver (Measurement-device-independent (MDI) QKD, twin-field (TF) QKD), one common entanglement-based transmitter to two receivers (Entanglement based QKD), shown in Figure 2.2.

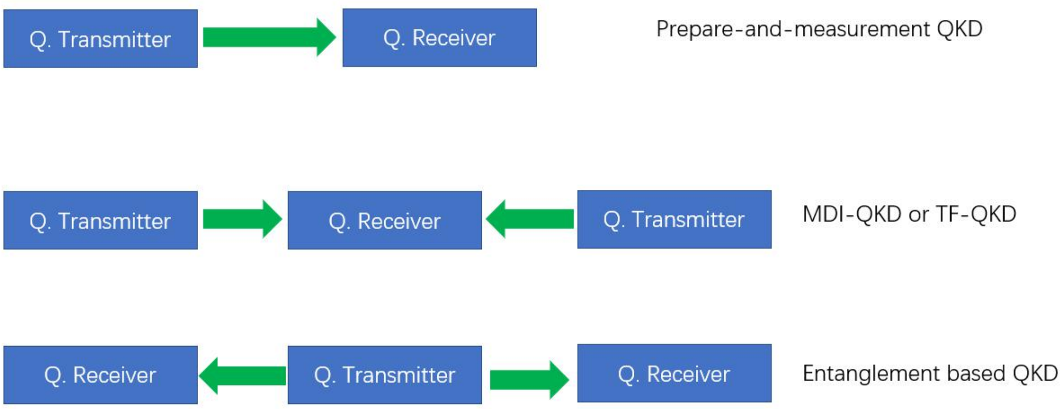
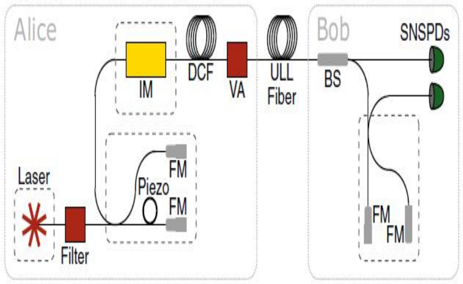
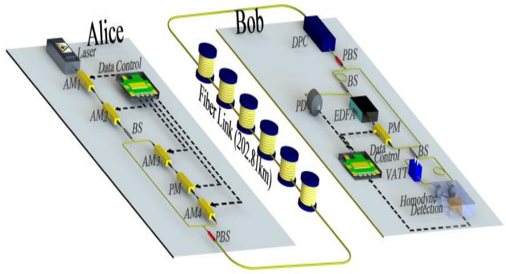


Figure 2.2 Types of QKD in terms of the behavior of Tx and Rx

The prepare-and-measurement QKD is most commercially matured one and it can be further divided into two types: DV-QKD and CV-QKD, as shown in Table 2-1.

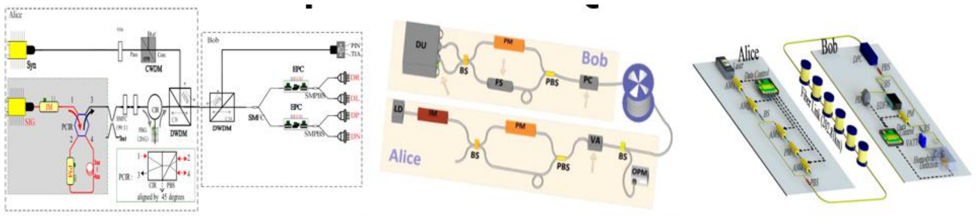
Table 2- 1 DV-QKD and CV-QKD, a comparison

Discrete Variable QKD (DV-QKD)	**Continuous Variable QKD (CV-QKD)**
• Maximum Baud rate at 1.25Ghz for product • Maximum Baud rate at 10Ghz record • Based on single photon detection • Degree of freedom: polarization, time bin + phase, frequency • Dark fiber preferred, good at high loss channel • Co- existence with data communication possible, low tolerance. • Relatively simple post-processing • Record from Univ.Geneva : 6.5bps@69.3dB	• Maximum Baud rate no more than 100Mhz for product • Maximum Baud rate around 1Ghz record • Based on coherent detection • Degree of freedom: In-phase component and quadrature of EM field • Dark fiber is not a must, good at low loss channel • Co- existence with data communication possible, high tolerance • Complex post-processing • Record from BUPT&PKU: 6.2bps@32.45 dB

 Alice IM DCF VA ULL Fiber Bob BS SNSPDs Laser Piezo FM FM Filter FM FM Phys. Rev. Lett. 121, 190502 (2018)	 Alice Bob Laser AM1 Data Control AM2 BS AM3 PM AM4 PBS Fiber Link (202.81km) DPC PBS BS PD EDFA PM Data Control VATT BS Homodyne Detection Phys. Rev. Lett. 125, 010502 (2020)

2.1.3 The Needed Optoelectronic Components of QKD and the Low-Cost Implementation

In Figure 2.3, The three typical QKD systems using photon’s physical degree of freedom are listed: DV-QKD Polarization, DV-QKD Time-Phase, CV-QKD Transmitted Local Oscillator (TLO). The source of high cost comes from the usage of Lithium niobate modulator, electric polarization controller, fiber-based Asymmetric MZI and single photon detector. Thanks to the rapid progress of silicon photonic chip and III-V material photonic chip development recent years, the QKD can benefit from low-cost device. In Figure 2.4, an example is shown how the tradition way of modulating the intensity and polarization of the quantum signal carrier can be shrink into a small device.



QKD Type	DV-QKD Polarization	DV-QKD Time-Phase	CV-QKD-TLO GG02
Typical Groups	Quantum Cteck, Univ.Padova	Toshiba (their old system)	BUPT，CNRS
Laser	🟩 DFB Laser	🟩 DFB Laser	🟨 Narrow linewidth Laser
Encoding/Modulation	🟨 LN Modulatorx2,Sagnac loop	🟨 LN modulatorx2，fiber-AMZI	🟥 LN modulatorx3~5，fiber-AMZI
Channel Control	🟨 Electric Pol.Controller	🟨 Electric Pol.Controller	🟨 Electric Pol.Controller
Decoding/De-modulation	🟨 Electric Pol.Controller	🟨 LN modulatorx1，fiber-AMZI	🟨 LN modulatorx1，fiber-AMZI
Optical signal detection	🟥 Single photon detectorx4	🟥 Single photon detectorx2~4	🟩 Homodyne detectorx1~2

🟥 Very High cost 🟨 High cost 🟩 Moderate cost

Figure 2.3 Cost issue with QKD system

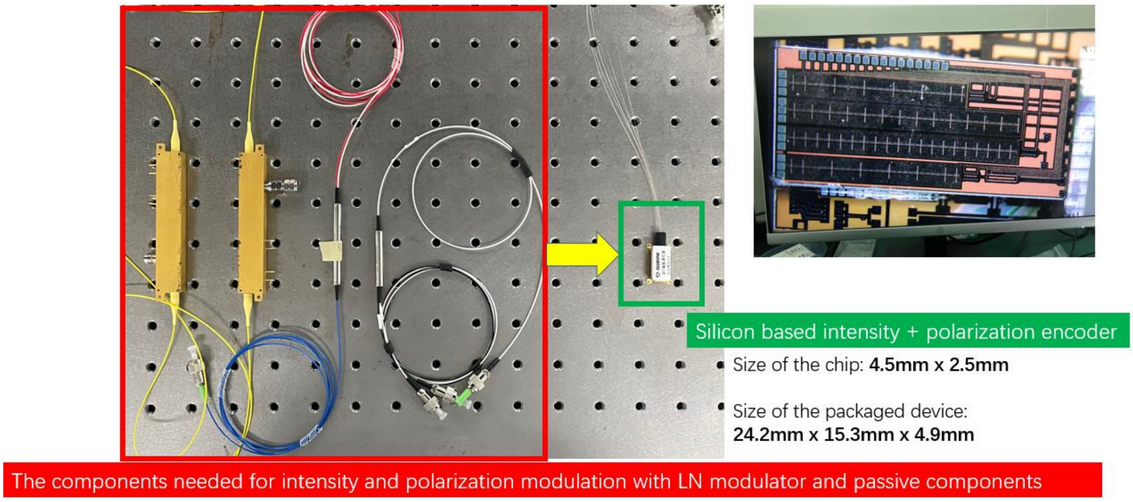

Silicon based intensity + polarization encoder
Size of the chip: 4.5mm x 2.5mm
Size of the packaged device:
24.2mm x 15.3mm x 4.9mm
The components needed for intensity and polarization modulation with LN modulator and passive components

Figure 2.4 Shrink the size of tradition component into a small device for QKD

With compact silicon photonics chip and III-V components (Figure 2.5) and application-specific integrated circuit (ASICs), the full optoelectronic functions can be packaged into a standard C form-factor pluggable (CFP) size module that is widely used in traditional optical communication industry, which implies standard and cost-effective QKD Tx module and QKD Rx module are feasible in the near future. Then the QKD functions can be realized via CFP QKD module with on-board computation electronics, this will benefit the implementation of quantum secure communication system in terms of size, cost and flexibility (Figure 2.6).

Figure 2.5 Compact III-V material based single photon detector

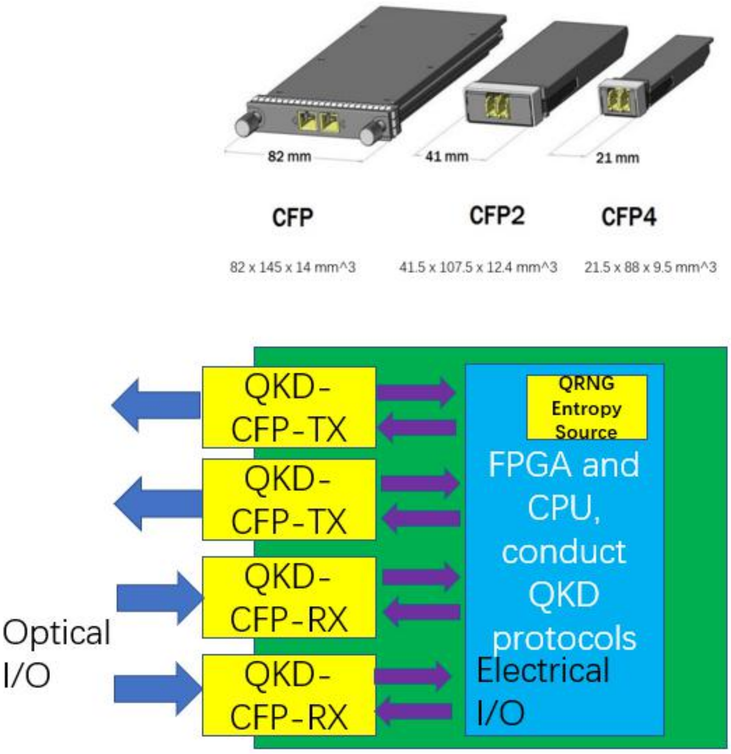


Figure 2.6 The future of standard CFP QKD module

2.2 Standardization Activities for QKDN

QKD and its networking technologies have attracted a lot of interest in multiple SDOs, e.g., ISO, IEC, ITU, IEEE, IETF, ETSI, as shown in 2.7. The status of Quantum Key Distribution Networks (QKDN) standardization in different SDOs will be briefly reviewed in the following sub-clauses.

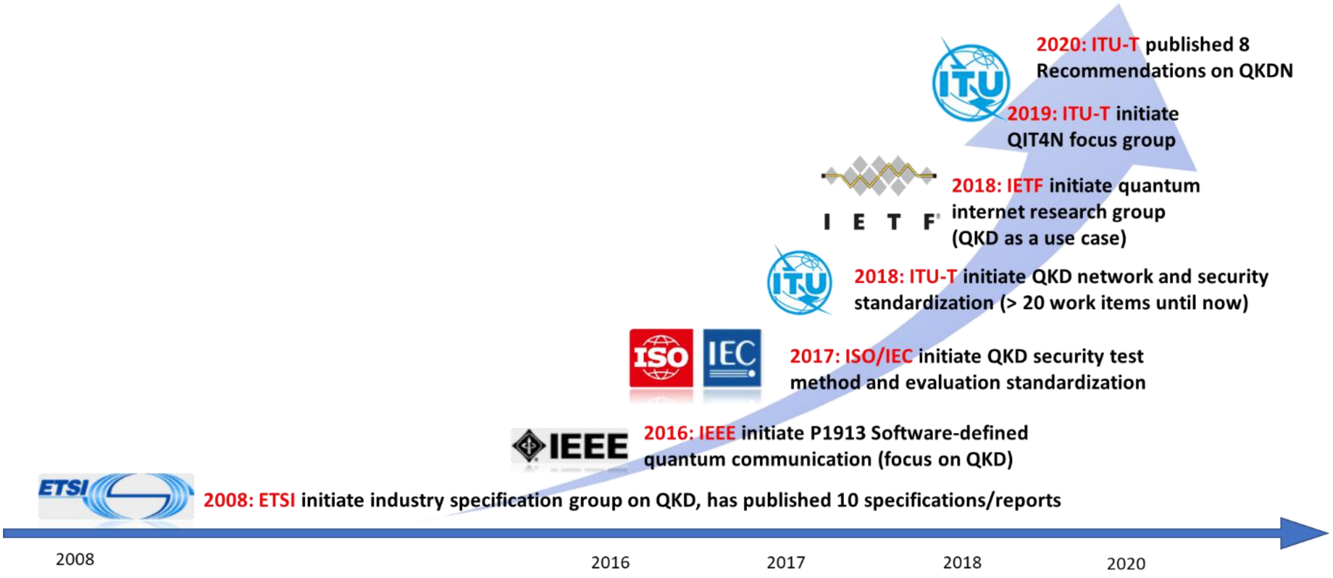

2020: ITU-T published 8 Recommendations on QKDN
2019: ITU-T initiate QIT4N focus group
2018: IETF initiate quantum internet research group (QKD as a use case)
2018: ITU-T initiate QKD network and security standardization (> 20 work items until now)
2017: ISO/IEC initiate QKD security test method and evaluation standardization
2016: IEEE initiate P1913 Software-defined quantum communication (focus on QKD)
2008: ETSI initiate industry specification group on QKD, has published 10 specifications/reports
2008
2016
2017
2018
2020

Figure 2.7 QKDN standardization timeline

2.2.1 ITU-T

ITU-T is the first SDO to standardize QKD as a network since 2018. At the time of this report's publication, ITU-T Study Groups 13 and 17 had cumulatively initiated 18 work items on the network and security and aspects of QKD networks, respectively.

2.2.1.1 ITU-T Study Group 11

At the time of this report's publication, SG11 had initiated 1 work items on QKDN for study, as listed in Table 2-2.

Table 2- 2: QKD related work items in ITU-T SG11

Q	Reference	Title	Type	Status
Q2/11	Q.QKDN_profr	Quantum key distribution networks – Protocol framework	Recommendation	Under development

2.2.1.2 ITU-T Study Group 13

At the time of this report's publication, SG13 had adopted 5 standards on QKDN, including the QKDN overview (Y.3800), functional requirements (Y.3801), functional architecture (Y.3802), key management (Y.3803), control and management (Y.3804) and initiated 17 work items on QKDN for study, as listed in Table 2-3.

Table 2- 3: QKD related work items in ITU-T SG13

Q	Reference	Title	Type	Status
Q16/13	Y.3800	Overview on networks supporting quantum key distribution	Recommendation	Published (2019-11)
Q16/13	Y.3801	Functional requirements for quantum key distribution network	Recommendation	Published (2020-07)
Q16/13	Y.3802	Quantum key distribution networks - Functional architecture	Recommendation	Published (2021-04)
Q16/13	Y.3803	Quantum key distribution networks - Key management	Recommendation	Published (2021-03)
Q16/13	Y.3804	Quantum Key Distribution Networks - Control and Management	Recommendation	Published (2021-01)
Q16/13	Y.3805	Quantum Key Distribution Networks - Software Defined Networking Control	Recommendation	Under development
Q6/13	Y.3806	Requirements for QoS Assurance of the Quantum Key Distribution Network	Recommendation	Under development
Q16/13	Y.Sup70	ITU-T Y.3800-series - Quantum key distribution networks	Supplement	Published (2021-09)

Q	Reference	Title	Type	Status
		- Applications of machine learning		
Q16/13	Y.QKDN_BM	Quantum Key Distribution Networks - Business role-based models	Recommendation	Under development
Q16/13	Y.QKDN_frint	Framework for integration of QKDN and secure storage network	Recommendation	Under development
Q16/13	Y.QKDN-iwfr	Quantum key distribution networks - interworking framework	Recommendation	Under development
Q16/13	Y.QKDN-ml-fra	Quantum Key Distribution Networks - Functional requirements and architecture for machine learning	Recommendation	Under development
Q6/13	Y.QKDN-qos-fa	Functional architecture of QoS assurance for quantum key distribution networks	Recommendation	Under development
Q6/13	Y.QKDN-qos-gen	General Aspects of QoS (Quality of Service) on the Quantum Key Distribution Network	Recommendation	Under development
Q6/13	Y.QKDN-qos-ml-req	Requirements of machine learning based QoS Assurance for quantum key distribution networks	Recommendation	Under development
Q16/13	Y.QKDN-rsfr	Quantum key	Recommendation	Under

Q	Reference	Title	Type	Status
		distribution networks - resilience framework		development
Q16/13	Y.supp.QKDN-roadmap	Standardization roadmap on Quantum Key Distribution Networks	Supplement	Under development

The structure of work on QKDN standardization in SG13 is illustrated in Figure 2.8.

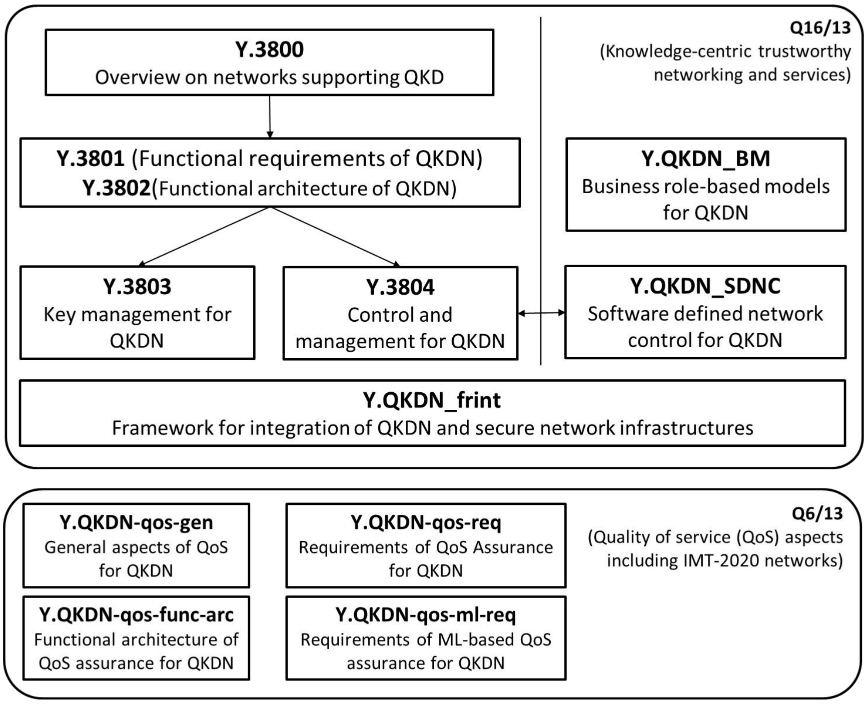

Q16/13
(Knowledge-centric trustworthy networking and services)
Y.3800
Overview on networks supporting QKD
Y.3801 (Functional requirements of QKDN)
Y.3802(Functional architecture of QKDN)
Y.QKDN_BM
Business role-based models for QKDN
Y.3803
Key management for QKDN
Y.3804
Control and management for QKDN
Y.QKDN_SDNC
Software defined network control for QKDN
Y.QKDN_frint
Framework for integration of QKDN and secure network infrastructures
Y.QKDN-qos-gen
General aspects of QoS for QKDN
Y.QKDN-qos-req
Requirements of QoS Assurance for QKDN
Q6/13
(Quality of service (QoS) aspects including IMT-2020 networks)
Y.QKDN-qos-func-arc
Functional architecture of QoS assurance for QKDN
Y.QKDN-qos-ml-req
Requirements of ML-based QoS assurance for QKDN

Figure 2.8: QKDN standardization work items in SG13

2.2.1.3 ITU-T Study Group 17

SG17 established a new Question, Q15/17, Security for/by emerging technologies including quantum-based security, approved by TSAG's September 2020 meeting. The Q15/17 terms of reference are available at [1].

At the time of this report's publication, SG17 had adopted 3 standards on QKDN and QRNG, including QKDN security framework (X.1710), key combination and confidential key supply

(X.1714) and QRNG architecture (X.1702), and initiated 10 work items on QKDN for study, as listed in Table 2-4.

Table 2- 4: QKD related work items in ITU-T SG17

Reference	Title	Type	Status
X.1702	Quantum noise random number generator architecture	Recommendation	Published (2019-11)
X.1710	Security framework for quantum key distribution networks	Recommendation	Published (2020-10)
X.1714	Key combination and confidential key supply for quantum key distribution networks	Recommendation	Published (2020-10)
XSTR-SEC-QKD	Security considerations for quantum key distribution network	Technical Report	Published (2020-03)
X.1712	Security requirements and measures for QKD networks - key management	Recommendation	Under development
X.sec_QKDN_AA	Authentication and authorization in QKDN using quantum safe cryptography	Recommendation	Under development
X.sec_QKDN_CM	Security requirements and measures for quantum key distribution networks - control and management	Recommendation	Under development
X.sec_QKDN_intrq	Security requirements for integration of QKDN and secure network infrastructures	Recommendation	Under development
X.sec_QKDN_tn	Security requirements for Quantum Key Distribution Networks - trusted node	Recommendation	Under development
TR.hybsec-qkdn	Technical Report: Overview of hybrid security approaches applicable to QKD	Technical Report	Under development

The structure of work on QKDN standardization in SG17 is illustrated in Figure 2.9.

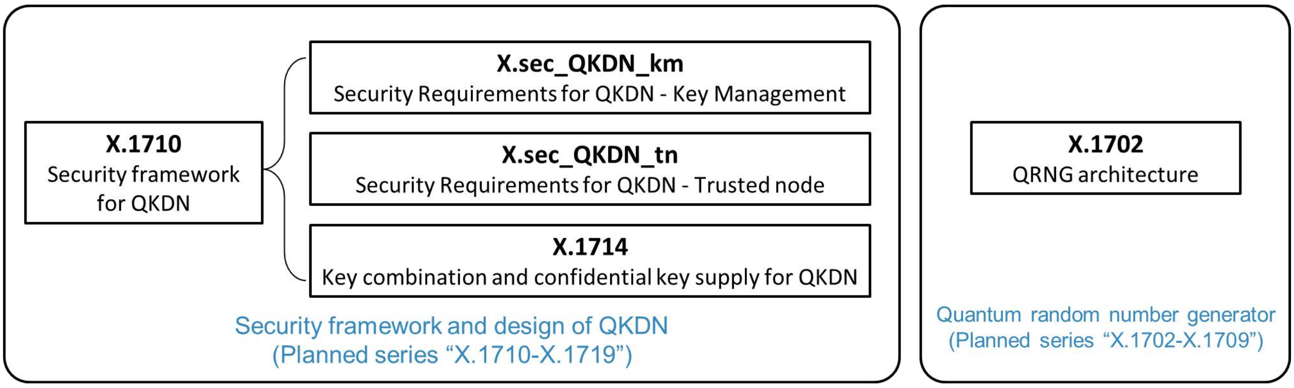

X.sec_QKDN_km
Security Requirements for QKDN - Key Management
X.1710
Security framework for QKDN
X.sec_QKDN_tn
Security Requirements for QKDN - Trusted node
X.1714
Key combination and confidential key supply for QKDN
Security framework and design of QKDN
(Planned series "X.1710-X.1719")
X.1702
QRNG architecture
Quantum random number generator
(Planned series "X.1702-X.1709")

Figure 2.9: QKDN standardization work items in SG17

2.2.2 ETSI ISG-QKD

ETSI initiated the industry specification group (ISG) on QKD in 2008. ETSI ISG-QKD has published nine specifications on QKD until 2019 and have several work items ongoing as listed in Table 2-5. The previous work mainly focused on QKD link-level issues, including QKD optical components, modules, internal and application interfaces, practical security, etc. Note that ETSI has also initiated the study of QKD network architectures recently and the specification of QKD security certification based on common criteria.

Table 2- 5: QKD related work items in ETSI

Reference	Title	Status
GS QKD 002	Quantum Key Distribution (QKD); Use Cases	Published (2010-06)
GR QKD 003	Quantum Key Distribution (QKD); Components and Internal Interfaces	Published (2018-03)
GS QKD 004	Quantum Key Distribution (QKD); Application Interface	Published (2010-12)
GS QKD 005	Quantum Key Distribution (QKD); Security Proofs NOTE – Revision in progress	Published (2010-12)
GR QKD 007	Quantum Key Distribution (QKD); Vocabulary	Published (2018-12)

Reference	Title	Status
	NOTE – Revision in progress	
GS QKD 008	Quantum Key Distribution (QKD); QKD Module Security Specification	Published (2010-12)
GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems	Published (2016-05)
GS QKD 012	Quantum Key Distribution (QKD) Device and Communication Channel Parameters for QKD Deployment	Published (2019-02)
GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of key delivery API to Applications;	Published (2019-02)
GS QKD 015	Quantum Key Distribution (QKD); Quantum Key Distribution Control Interface for Software Defined Networks	Published (2021-03)
DGS/QKD-0010_ISTrojan	Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems	Under development
DGS/QKD-0013_TransModChar	Quantum Key Distribution (QKD); Characterisation of Optical Output of QKD transmitter modules	Under development
DGS/QKD-016-PP	Quantum Key Distribution (QKD); Common Criteria Protection Profile for QKD	Under development
DGR/QKD-017NwkArch	Quantum Key Distribution (QKD); Network architectures	Under development
DGS/QKD-018OrchIntSDN	Quantum Key Distribution (QKD); Orchestration Interface of Software Defined Networks	Under development

2.2.3 ISO/IEC JTC 1/SC 27

ISO/IEC JTC 1/SC 27 initiated the study period "Security requirements, test and evaluation methods for quantum key distribution" in 2017. In 2019, the study period was completed, and a new work item ISO/IEC 23837 (Part 1&2) was established as listed in Table 2-6.

Table 2- 6: QKD related works items in ISO/IEC JTC1

Reference	Title	Status
ISO/IEC 23837-1	Security requirements, test and evaluation methods for quantum key distribution Part 1: requirements	Under development
ISO/IEC 23837-2	Security requirements, test and evaluation methods for quantum key distribution Part 2: test and evaluation methods	Under development

2.3 Implications for 6G

2.3.1 State-of-the-art of QKD in 5G

In 5G era, the importance of cybersecurity in mobile communications will rise exponentially. Quantum cryptography has emerged as a potential solution for safeguarding critical information because it is impossible to copy data encoded in a quantum state. Some mobile operators have applied encryption technology using QKD to 5G networks, for example, in April 2021, SK Telecom (SKT) and its subsidiary ID Quantique (IDQ), a Geneva-based leader in quantum-safe cryptography, have developed a quantum virtual private network (VPN) based on the QKD. VPN is a secured communications channel implemented over shared, public networks to connect remote users and machines to a private network. QKD is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics [2]. In 6G, with the development of technology, it matures day by day.

In order to resist the potential impact on the classic cryptography system, 256 bits algorithms will be endorsed to replace the 128 bits algorithms. In 5G, the 128 bits algorithms NR Integrity Algorithm (NIA)/NR Encryption Algorithm (NEA) 1/2/3 are used for the Access Stratum (AS) and Non-Access Stratum (NAS) security protection based on the shared key, meanwhile the corresponding 256 bits algorithms are already under investigation in 3GPP SA3 and ETSI

Security Algorithms Group of Experts (SAGE). The new 256 bits algorithms will probably be introduced in 6G era. AES-256 will be one of the candidates, even with currently known quantum algorithms like Grover's, National Institute of Standards and Technology (NIST) believes that AES 256 keys will still be safe for a very long time and recommends that current applications can continue to use AES with key sizes 128, 192, or 256 bits [3].

For asymmetric algorithms, e.g., Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI), RSA, they are widely used in 5G system and Internet services. NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. It is intended that the new public-key cryptography standards will specify one or more additional unclassified, publicly disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers. It was planned to get the draft standards on Post-Quantum Cryptography (PQC) available at 2022-2024. This is the most critical issue to standardize the most stable and secure PQC before deploying them into the 6G. Early adoption of post quantum algorithms would be both very complex, and yet result in potentially uncertain security guarantees.

2.3.2 Integration of 6G and QITs

The composition of 6G network requires high-precision data capability, computing capability and security, which can be enabled by quantum technologies such as quantum precision measurement, quantum computing and quantum communication.

(1) Quantum computing will help 6G maximize spectrum utilization and improve resource allocation efficiency.

In the 6G era, the wireless industry may re-examine the traditional spectrum allocation mechanism and further evolve the dynamic spectrum sharing technology. Through the use of

Artificial Intelligence, Blockchain and other technologies, more intelligent and dynamic spectrum allocation, control and scheduling can be realized to maximize spectrum utilization. Quantum computing will achieve optimal wireless resource allocation and cell planning and improve energy efficiency and spectrum efficiency.

(2) Quantum private communication technology ensures network data security and supports the development of digital economy.

Traditional cryptography based on computational complexity will face the threat of quantum computer attacks in the 6G era. Enhanced cryptography such as quantum key and wireless physical layer key will provide a stronger security guarantee for 6G. In the future, 6G networks will rely on lightweight access authentication, quantum key, blockchain and other advanced security technologies to provide active defense for network infrastructure.

2.3.3 Typical Application Scenarios of QKD

Quantum encrypted communication can be applied to protect the data acquisition and processing system of infrastructure, ensuring the security of data communication. It can be widely used in frontier fields such as digital twins, smart parks, blockchains and so on.

Taking the management and scheduling of the smart park as an example, collect and analyze the environmental information of the park through sensing equipment (camera, radar), roadside unit and positioning reference station, and build a business system based on 'vehicle-road-human-cloud collaboration’, which can realize the efficient and fast management of personnel, materials and equipment in the park. The collected data is closely related to the management ability of the park, and its authenticity and integrity can be protected by quantum key distribution.

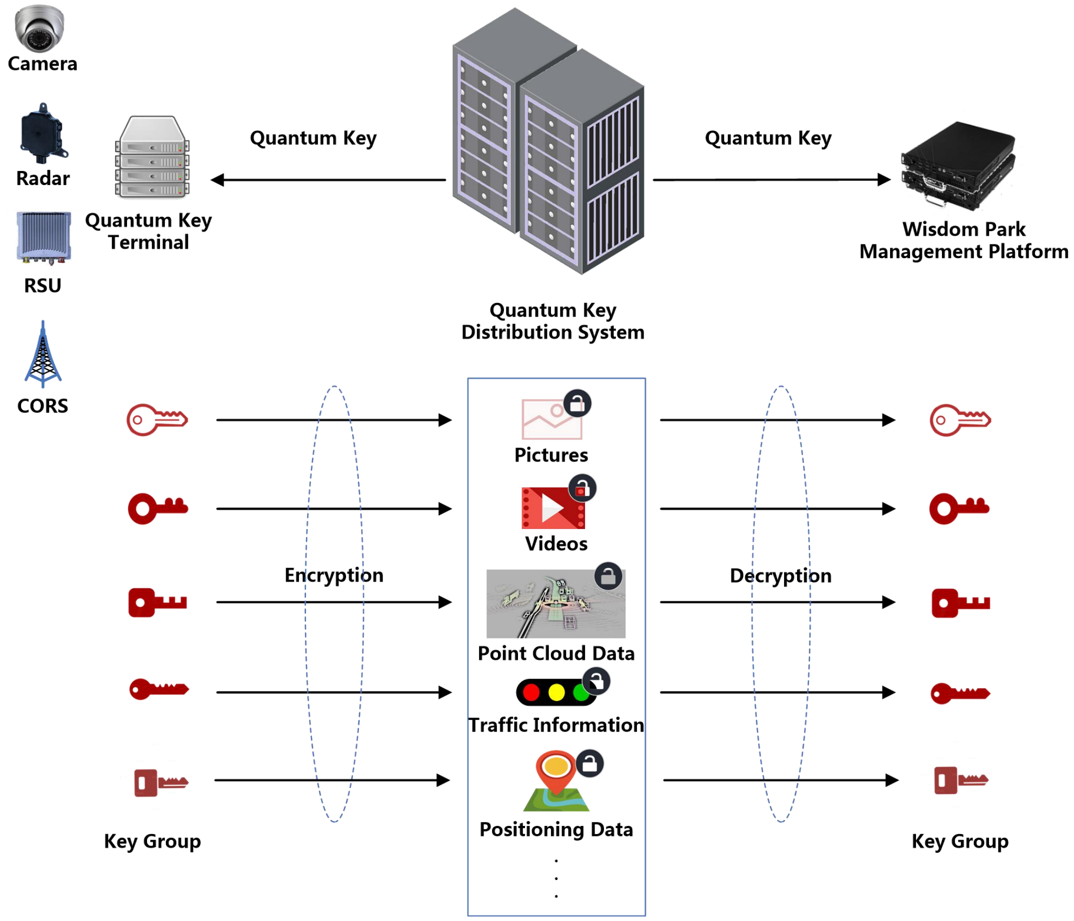


Figure 2.10 Data Encryption of Smart Park Based on Quantum Security System

Data transmission with the quantum encryption system is shown in the Figure 2.10. The quantum key distribution system provides keys for reliable authentication and data encryption of video, pictures, point cloud data, traffic information, location information and other data of the park. The quantum key distribution system can also change the key according to the specific business requirements, realizing the intelligent management of the park and secure data transmission. In the future, the quantum encryption system will be applied to the construction of Winter Olympics Smart Park and Xiong'an New Area.

For example, in Xiong’an quantum communication pilot as illustrated by Figure 2.11, a quantum communication trunk line between Beijing and Xiong’an will be deployed, and a quantum key distribution platform will be introduced to provide security keys for customers in the fields of Internet of things (IoT), Internet of vehicles (IoV), smart energy, smart government and so on. The quantum key distribution platform and the service application server can be deployed together without changing the original network topology, and the encrypted business is still transmitted in the original service channels.

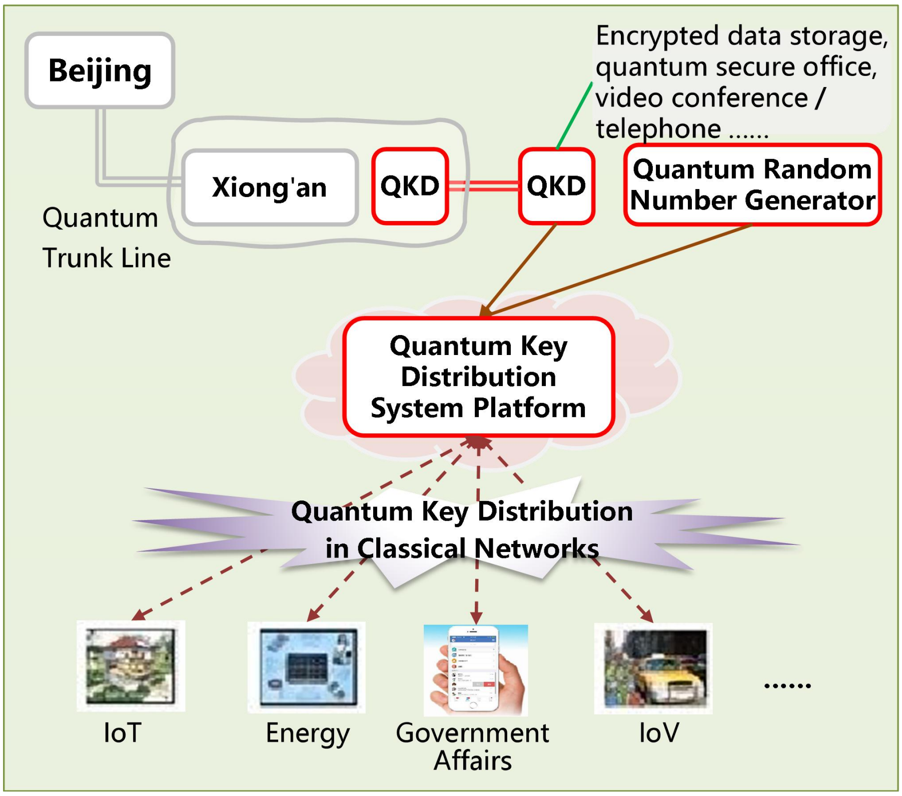

Beijing
Encrypted data storage, quantum secure office, video conference / telephone ......
Xiong'an
QKD
QKD
Quantum Random Number Generator
Quantum Trunk Line
Quantum Key Distribution System Platform
Quantum Key Distribution in Classical Networks
IoT
Energy
Government Affairs
IoV
......

Figure 2.11 Quantum Communication Pilot in Xiong'an

3 Quantum Machine Learning (QML)

It is highly expected that the 6th generation (6G) communication systems will lay a foundation of pervasive digitization, ubiquitous connection and full intelligence. The provisions of a many-fold increase in the communication system performance and rich diversity of innovative services call for a revolutionary promotion in information processing capability. In this regard, the emerging Quantum Machine Learning (QML) has attracted significant attention due to its information processing paradigm by combining the established benefits of quantum mechanism and machine learning. In the following, we start with the concepts of QML on a high level and then discuss machine learning (ML) basic paradigms and their application in solving problem across different layers of in communication systems. Followed by introduction of quantum tools, we present examples to get insight into the research of QML. Consequently, QML for communication systems can be obtained by ML for communication system being synergy with quantum speedup.

QML is the integration of quantum algorithms within machine learning programs, and thus achieving quantum speedup. Therefore, QML can generate and recognize statistical data patterns that are beyond the capabilities of computing or machine learning in the classical domain [4]. On a high level, the concepts of QML can be categorized into the following three tiers [5].

- Tier 1. The most common use of the term refers to machine learning algorithms for the analysis of classical data executed on a quantum computer, i.e. *quantum-enhanced machine learning*. While machine learning algorithms are used to compute immense quantities of data, quantum machine learning utilizes qubits and quantum operations or specialized quantum systems to improve computational speed and data storage done by algorithms in a program. This includes hybrid methods that involve both classical and quantum processing, where computationally difficult subroutines are outsourced to a quantum device. These routines can be more complex in nature and executed faster on a quantum computer.

- Tier 2. Quantum algorithms can be used to analyze quantum states instead of classical data. The term "quantum machine learning" is also associated with classical machine learning methods applied to data generated from quantum experiments (i.e. *machine learning of quantum systems*), such as learning the phase transitions of a quantum system or creating new quantum experiments.
- Tier 3. Quantum machine learning also extends to a branch of research that explores methodological and structural similarities between certain physical systems and learning systems. For example, some mathematical and numerical techniques from quantum physics are applicable to classical deep learning and vice versa. Furthermore, researchers investigate more abstract notions of learning theory with respect to quantum information, sometimes referred to as "*quantum learning theory*".

3.1 Machine Learning for Communication Systems

Machine learning technologies are conventionally regarded as comprising of three basic paradigms, i.e., supervised learning, unsupervised learning and reinforcement learning. This section gives a brief introduction of applying the above three paradigms in solving a wide range of problems across different layers of communication systems, as illustrated in Table 3-1.

Table 3- 1 Example applications of ML in different layers of communicaiton system

	Supervised	Unsupervised	Reinforcement
PHY and MAC	• Channel model generation • Signal processing • Power allocation and interference cancellation • CSI estimation	• Spectrum sensing • Multiple access • Location • Beam management	• On-demand resource (power, radio resources) optimization • Transmission mode selection • Admission control
Network	• Traffic classification • Caching	• Network anomaly detection • Traffic prediction • Optimized routing • Network state/parameters	• Proactive caching • Traffic prediction and classification • Optimized routing

		prediction	

Supervised Learning is a machine learning task to infer a function that maps an input object to a desired output based on example input-output pairs, where the example input-output pairs are referred to as labeled training data such as obtained from domain knowledges [6]. Supervised learning is typically used to solve classification and regression problems. Therefore, supervised learning can play an important role in channel model generation, signal processing, and so on.

Unsupervised Learning is a machine learning task that learns patterns from unlabeled data [7]. Additionally, if a small amount of labeled training data is available, the machine learning task is called semi-supervised learning. Here we will avoid these details and only take unsupervised learning for instance to do discussion. Some of the most common algorithms used in unsupervised learning include clustering, anomaly detection and approaches for learning latent variable models. In contrast to supervised learning, unsupervised learning has no dependence of labeled data and thus can be applied for clustering or tracking in a fast time-varying environment. Unsupervised learning can potentially be applied for clustering or pairing of network nodes or endpoints for the purposes of optimal allocation of various resources, particularly in a vehicle-to-everything (V2X) communication system.

Reinforcement Learning (RL) [8] is an area of machine learning concerned with how intelligent agents react in an environment with a target of maximizing the reward. The focus of RL is on finding a balance between exploration (of uncharted territory) and exploitation (of current knowledge) [9]. As compared to supervised learning, labeled training data is not required for reinforcement learning. However, partially supervised RL algorithms can combine the advantages of supervised and RL algorithms. One powerful feature of RL is suitable for dealing with large environments. Reinforcement learning is typically used for solving control and classification problems. Conventional and notable RL algorithms such as Q-learning and multi-armed bandit take as an input the current state of the network and enable the prediction of the next state. A promising application of RL in communication contributes to scheduling parameters optimization across various layers. Additionally, deep learning can be combined with RL to facilitate learning long-term temporal dependence sequences in such a way that the accumulation of errors won’t grow very fast [10].

3.2 Quantum Tools

This section revisits some principles and concepts associated with quantum mechanism, which will be referred to in the succeeding introduction of QML.

Quantum entanglement [11] is a physical phenomenon that occurs when a group of particles are generated, interact, or share spatial proximity in a way such that the quantum state of each particle of the group cannot be described independently of the state of the others, including when the particles are separated by a large distance. The topic of quantum entanglement is at the heart of the disparity between classical and quantum physics: entanglement is a primary feature of quantum mechanics lacking in classical mechanics.

Quantum superposition [12] is a fundamental principle of quantum mechanics. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct states. Mathematically, it refers to a property of solutions to the Schrödinger equation; since the Schrödinger equation is linear, any linear combination of solutions will also be a solution.

Quantum simulators [13] permit the study of quantum system in a programmable fashion. In this instance, simulators are special purpose devices designed to provide insight about specific physics problems. Quantum simulators may be contrasted with generally programmable "digital" quantum computers, which would be capable of solving a wider class of quantum problems. Quantum simulators have been realized on a number of experimental platforms, including systems of ultracold quantum gases, polar molecules, trapped-ions, photonic systems, quantum dots, and superconducting circuits.

3.3 QML for Communication Systems

This section presents examples to get insight into the research of QML from three tiers, i.e., quantum-enhanced machine learning, machine learning of quantum systems and quantum learning theory. Being synergy with the aforementioned machine learning (ML) basic paradigms and their application in the context of communication, we can obtain QML for communication systems.

3.3.1 Quantum-enhanced Machine Learning

Quantum-enhanced supervised and unsupervised learning

The work in [14] provides supervised and unsupervised quantum machine learning algorithms for cluster assignment and cluster finding, which proves that QML can take time logarithmic in both the number of vectors and their dimension, therefore providing an exponential speed-up over classical ML algorithms. It is described in [15] a quantization method which refers to the process that partially or totally converts a classical algorithm to its quantum counterpart in order to accelerate learning algorithms. In particular, the quantized routines employed for learning algorithms that translate into an unstructured search task is done by k-medians.

Quantum-enhanced reinforcement learning

In quantum-enhanced reinforcement learning, a quantum agent interacts with a classical or quantum environment and occasionally receives rewards for its actions, which allows the agent to learn what to do in order to gain more rewards. There are various ways of achieving quantum speedup. For example, in [16] a quantum agent which has quantum processing capability is provided in achieving a quadratic speed-up for active learning. Alternatively, the work in [17] gains speed-up by probing the environment in superpositions**.** Furthermore, a general method of quantum improvements in three paradigms of machine learning is provided in [17]. A quantum speedup of the agent's internal decision-making time has been experimentally demonstrated in trapped-ions [18], while a quantum speedup of the learning time in a fully coherent (`quantum') interaction between agent and environment has been experimentally realized in a photonic setup

[19].

In order to make the QML for communications a reality, powerful simulators of quantum devices are required to facilitate development of QML algorithms. However, the quantum computers simulators available today can only simulate a small number of circuits, because the simulation of a quantum computer on a classical computer is a computationally hard problem. In parallel, the development of quantum devices (sensors, measurement, etc) with a high degree of precision and sensitivity is crucial not only for facilitating the development QML algorithms but also for exploitation of quantum mechanism concepts and principles.

3.3.2 Machine Learning of Quantum Systems

The work in [20] shows an experiment performed to reconstruct an unknown photonic quantum state with a limited amount of copies. In particularly, a semi-quantum reinforcement learning approach is employed to adapt one qubit state, an "agent," to an unknown quantum state, an "environment," by successive single-shot measurements and feedback, in order to achieve maximum overlap. The experimental learning device herein, composed of a quantum photonics setup, can adjust the corresponding parameters to rotate the agent system based on the measurement outcomes "0" or "1" in the environment (i.e., reward/punishment signals).

3.3.3 Quantum Learning Theory

Quantum learning theory [4] pursues a mathematical analysis of the quantum generalizations of classical learning models and of the possible speed-ups or other improvements that they may provide. The framework is very similar to that of classical computational learning theory, but the learner in this case is a quantum information processing device, while the data may be either classical or quantum. Quantum learning theory should be contrasted with the quantum-enhanced machine learning discussed above, where the goal was to consider specific problems and to use quantum protocols to improve the time complexity of classical algorithms for these problems. Quantum learning theory is still under development.

The fundamental in learning theory is a concept class, each of which is usually a function on some domain. The goal for the learner is to learn (exactly or approximately) an unknown target concept from this concept class. The learner may be actively interacting with the target concept, or passively receiving samples from it. In active learning, a learner can make membership queries to the target concept c, asking for its value c(x) on inputs x chosen by the learner. The learner then has to reconstruct the exact target concept, with high probability. In passive learning, the learner receives random examples (x,c(x)), where x is distributed according to some unknown distribution D. The goal of the learner is to output a hypothesis function h such that h(x)=c(x) with high probability when x is drawn according to D.

4 Reference

[1] https://itu.int/en/ITU-T/studygroups/2017- 2020/17/Pages/q15.aspx

[2] https://www.ajudaily.com/view/20210406110320727

[3] “Post-Quantum Cryptography - FAQs.” NIST Computer Security Resource Center, 6 Aug 2019, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs

[4] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary and M. Asaduzzaman, "Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future," in IEEE Access, vol. 7, pp. 46317-46350, 2019, doi: 10.1109/ACCESS.2019.2909490.

[5] https://en.wikipedia.org/wiki/Quantum_machine_learning

[6] https://en.wikipedia.org/wiki/Supervised_learning

[7] https://en.wikipedia.org/wiki/Unsupervised_learning

[8] https://en.wikipedia.org/wiki/Reinforcement_learning

[9] Leslie Pack Kaelbling, Michael L. Littman, and Andrew W. Moore. 1996. "Reinforcement learning: a survey," in Journal of Artificial Intelligence Research. 4, 1 (Jnauary 1996), 237–285.

[10]U. Challita, L. Dong and W. Saad, "Proactive Resource Management for LTE in Unlicensed Spectrum: A Deep Learning Perspective," in IEEE Transactions on Wireless Communications, vol. 17, no. 7, pp. 4674-4689, July 2018, doi: 10.1109/TWC.2018.2829773.

[11]https://en.wikipedia.org/wiki/Quantum_entanglement

[12]https://en.wikipedia.org/wiki/Quantum_superposition

[13] https://en.wikipedia.org/wiki/Quantum_simulator#Trapped-ion_simulators

[14] S. Lloyd, M. Mohseni, and P. Rebentrost, “Quantum algorithms for supervised and unsupervised machine learning,”, 2013.

[15] E. Aïmeur, G. Brassard, and S. Gambs, “Quantum speed-up for unsupervised learning,” Machine Learning, vol. 90, no. 2, pp. 261–287, 2013.

[16] Paparo, Giuseppe Davide; Dunjko, Vedran; Makmal, Adi; Martin-Delgado, Miguel Angel; Briegel, Hans J. (2014). "Quantum Speedup for Active Learning Agents". Physical Review

X. 4 (3): 031002.

[17] Dunjko, Vedran; Taylor, Jacob M.; Briegel, Hans J. (2016-09-20). "Quantum-Enhanced Machine Learning". Physical Review Letters. 117 (13): 130501.

[18] Sriarunothai, Theeraphot; Wölk, Sabine; Giri, Gouri Shankar; Friis, Nicolai; Dunjko, Vedran; Briegel, Hans J.; Wunderlich, Christof (2019). "Speeding-up the decision making of a learning agent using an ion trap quantum processor". Quantum Science and Technology. 4 (1): 015014.

[19] Saggio, Valeria; Asenbeck, Beate; Hamann, Arne; Strömberg, Teodor; Schiansky, Peter; Dunjko, Vedran; Friis, Nicolai; Harris, Nicholas C.; Hochberg, Michael; Englund, Dirk; Wölk, Sabine; Briegel, Hans J.; Walther, Philip (10 March 2021). "Experimental quantum speed-up in reinforcement learning agents". Nature. 591 (7849): 229–233.

[20] Yu, Shang; Albarran-Arriagada, F.; Retamal, J. C.; Wang, Yi-Tao; Liu, Wei; Ke, Zhi-Jin; Meng, Yu; Li, Zhi-Peng; Tang, Jian-Shun (2018-08-28). "Reconstruction of a Photonic Qubit State with Quantum Reinforcement Learning". Advanced Quantum Technologies. 2 (7–8): 1800074.

Acknowledgement

Grateful thanks to the following contributors for their wonderful work on this whitepaper:

Editors: Chih-Lin I (China Mobile), Xin GUO(Lenovo)

Contributors:

China Information and Communication Technologies Group Corporation (CICT) & National Information Optoelectronics Innovation Center (NOEIC)	Yi QIAN
University of Science and Technology Beijing (USTB)	Zhangchao MA, Jianquan WANG, Lei SUN
Apple	Shu GUO
China Unicom	Qi Liu，Meng Song，Chuanxin Zeng，Xingrong Xu
Lenovo	Xin GUO

Abbreviation

AS	Access Stratum
ASIC	Application-Specific Integrated Circuit
CFP	C Form-factor Pluggable
CV	Continuous Variable QKD
DV	Discrete Variable QKD
ECCSI	Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption
IDQ	ID Quantique
IoT	Internet of Things

IoV	Internet of Vehicles
ISG	Industry Specification Group
MDI	Measurement-Device-Independent
ML	Machine Learning
NAS	Non-Access Stratum
NEA	NR Encryption Algorithm
NIA	NR Integrity Algorithm
NIST	National Institute of Standards and Technology
POC	Post-Quantum Cryptography
QIT	Quantum Information Technology
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QML	Quantum Machine Learning
RL	Reinforcement Learning
SAGE	Security Algorithms Group of Experts
SDO	Standard Developing Organization
SKT	SK Telecom
TF	Twin-Field
TLO	Transmitted Local Oscillator
V2X	Vehicle-to-Everything
VPN	Virtual Private Network

FuTURE FORUM is committed to cutting edge technologies study and applications. Controversies on some technical road-maps and methodologies may arise from time to time. FuTURE FORUM encourages open discussion and exchange of ideas at all levels. The White Paper released by FuTURE FORUM represents the opinions which were agreed upon by all participating organizations and were supported by the majority of FuTURE FORUM members. The opinions contained in the White Paper does not necessarily represent a unanimous agreement of all FuTURE FORUM members.

FuTURE FORUM welcomes all experts and scholars' active participation in follow-on working group meetings and workshops. we also highly appreciate your valuable contribution to the FuTURE White Paper series.