International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(24 November 2021)

ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N)

FG QIT4N D2.5

Standardization outlook and technology maturity: Quantum key distribution network

ITU-T

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

Quantum information technology (QIT) is a class of emerging technology that improves information processing capability by harnessing principles of quantum mechanics which is expected to have a profound impact to ICT networks.

The ITU Telecommunication Standardization Advisory Group established the ITU-T Focus Group on Quantum Information Technology for Networks (FG QIT4N) in September 2019 to provide a collaborative platform to study the pre-standardization aspects of QITs for ICT networks.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

FG QIT4N concluded and adopted all its Deliverables as technical reports on 24 November 2021.

Number	**Title**
FG QIT4N D1.1	QIT4N terminology: Network aspects of QITs
FG QIT4N D1.2	QIT4N use cases: Network aspects of QITs
FG QIT4N D1.4	Standardization outlook and technology maturity: Network aspects of QITs
FG QIT4N D2.1	QIT4N terminology: QKDN
FG QIT4N D2.2	QIT4N use cases: QKDN
FG QIT4N D2.3	QKDN protocols: Quantum layer
FG QIT4N D2.3	QKDN protocols: Key management layer, QKDN control layer and QKDN management layer
FG QIT4N D2.4	QKDN transport technologies
FG QIT4N D2.5	Standardization outlook and technology maturity: QKDN

The FG QIT4N Deliverables are available on the ITU webpage, at https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx.

For more information about FG QIT4N and its deliverables, please contact tsbfgqit4n@itu.int.

Technical Report FG QIT4N D2.5

Standardization outlook and technology maturity: 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).

It provides an overview of quantum key distribution (QKD) technology, including frontier research, system experiment, field trial, and commercialized product. It conducts a summary of QKD industry status, including market players such as system vendor, network provider, and end user, project and opinions from different country and region, and other aspects. It contains QKD network standardization landscape, conducts gap analysis, and provides future standardization suggestions.

Note

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

Keywords

QKD; quantum key distribution; quantum key distribution network; industry; standardization.

Disclaimer

Sample projects, reference articles, specific companies, products or services mentioned in this report are only for the purposes of illustrating the technological maturity of QKDN. Their mention does not imply that they are endorsed or recommended by ITU, ITU's Secretariat, the Focus Group or the editors of this report, in preference to others of a similar nature that are not mentioned.

Chief editor: Junsen Lai
China Academy of Information and Communications Technology (CAICT)
China
Email: laijunsen@caict.ac.cn

Co-editors: Zhangchao Ma
CAS Quantum Network
China
Email: mazhangchao@qtict.com

Yi Qian
China Information and Communication Technologies Group Corporation (CICT)
China
Email: qianyi@cict.com

Acknowledgments

The editors express their appreciation to all the contributors of this report and all participants of Working Group 2 of the Focus Group on Quantum Information Technology for Networks (FG QIT4N) for their invaluable inputs, thorough review and all comments provided during the development of this report.

Table of Contents

Technical Report ITU-T FG QIT4N D2.5

Standardization outlook and technology maturity: Quantum key distribution network

1 Scope

This Technical Report studies standardization outlook and technology maturity of the Quantum Key Distribution (QKD) network. In particular, the scope of this draft technical report includes:

– Overview of QKDN technologies and industry development;

– Assessment of QKDN technologies maturity;

– QKDN standardization landscape and gap analysis;

– Outlook of QKDN standardization.

2 References

None.

3 Terms and definitions

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

APD	Avalanche Photodiodes
BSM	Bell-State Measurement
CV	Continuous Variable
DF	Dark Fibre
DV	Discrete Variable
GEO	Geostationary Orbit
IQP	Integrated Quantum Photonics
KM	Key Management
LEO	Low Earth Orbit
LF	Lit Fibre
LO	Local Oscillator
MDI	Measurement Device Independent
OTN	Optical Transport Network
OTP	One-Time Pad
P&M	Prepare and Measure
PDC	Parametric Down Conversion
PQC	Post-Quantum Cryptography
QAM	Quadrature Amplitude Modulation

QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QRNG	Quantum Random Number Generation
QSC	Quantum-Safe Cryptography
R&D	Research and Development
RRDPS	Round-Robin Differential Phase-Shift
SDN	Software Defined telecommunication Networks
SDO	Standards Developing Organization
SECoQC	Secure Communication based on Quantum Cryptography
SPD	Single-Photon Detector
SNSPD	Superconducting Nanowire Single-Photon Detector
SNU	Shot Noise Unit
SPAD	Single-Photon Avalanche Photodiodes
T&E	Testing and Evaluation
TF	Twin-field
ULL	Ultra-Low Loss
WDM	Wavelength-Division Multiplexing

5 Technology overview

5.1 Frontier research and exploration

Quantum key distribution (QKD) modules are core components of a quantum key distribution network (QKDN). Some frontier research in quantum communications and QKD may have an impact on QKD systems and the way they are interconnected such as chip-based QKD, satellite-based QKD and quantum repeaters. Reviewing the development and trends in these frontier research topics will contribute to the understanding of the maturity of QKDN technology.

5.1.1 Chip-based QKD

Integrated quantum photonics (IQP) technology has enabled the generation, processing and detection of quantum states of light at a steadily increasing scale and level of complexity. IQP has progressed from few-component circuitry occupying centimetre-scale footprints and operating on two photons, to programmable devices [b-Wang-1]. The deployment of a global quantum communication network will require new levels of sophistication to the manufacture of quantum technologies with a larger number of components. In exploiting single photons of light as quantum information carriers with wafer-scale fabrication processes, IQP is a compelling platform for the future of quantum technologies.

QKD aims to share symmetric keys between the transmitter and receiver based on the law of quantum mechanics, such that the achieved security is inaccessible by classical communications [b-Gisin]. Integrated photonics is a well-established technology developed and deployed in the global telecommunication industry. As such, it is natural to use integrated photonics for practical QKD applications to generate encrypted keys. Integrated photonics technology promises to enable a robust, miniaturized, and low-cost platform to realize QKD transmitters and receivers.

Pioneer studies began in 2004 with silicon dioxide (SiO_2)-based optical interferometers fabricated for time-bin QKD systems in fibre [b-Honjo]. However, the first fully integrated chip-to-chip QKD system was implemented with an indium phosphide (InP) transmitter chip and a silicon oxynitride (SiO_xN_y) receiver chip [b-Sibson-1]. The InP QKD transmitter incorporates all the necessary components such as a tuneable laser, attenuator, and electro-optic phase modulators (EOPM), the SiO_xN_y QKD receiver consists of thermo-optic phase shifters, which allow for digitally reconfigurable delay line and state measurement and photons were detected by off-chip superconducting nanowire single-photon detector (SNSPDs). These transceivers provide a complete chip-to-chip QKD solution, and could be programmed to implement multiple protocols, including BB84 at a 560 MHz state rate, coherent-one-way operating at an 860 MHz state rate, and differential phase shift at a 1.76 GHz state rate. Figure 1 illustrates the chip-to-chip QKD transceiver solution.

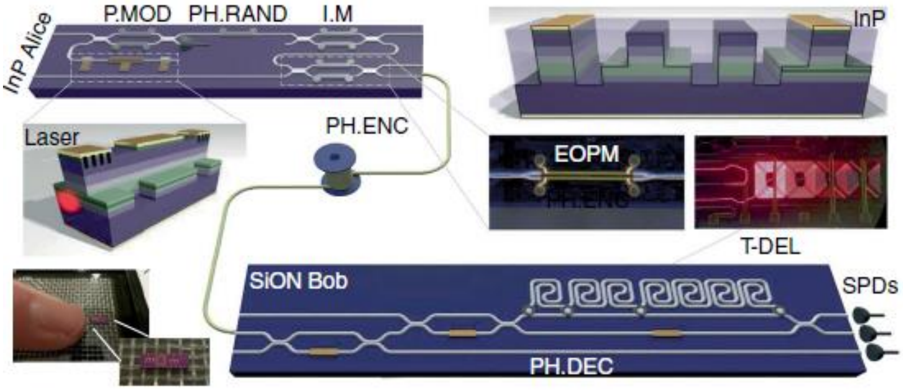


Figure 1 – Chip to chip QKD system between a 2×6 mm^2 InP transmitter and a 2×32 mm^2 SiO_xN_y receiver [b-Sibson-1]

Silicon photonics is an appealing technology platform for QKD applications due to its cost-effective manufacturing and compatibility with CMOS electronics. Even though fast manipulation of single photons in Si is challenging due to the lack of efficient electro-optic modulation and loss is high, the carrier injection or depletion modulation allows sufficient state preparation for QKD from a MHz to GHz rate. Recently, three groups have demonstrated Si-based QKD transmitters:

- transmitter which prepares polarization-encoded qubits for a BB84 system over a 5 km fibre [b-Ma];
- two transmitters were developed by [b-Sibson-2], one for polarization-encoded and the other for time-bin-encoded BB84 systems; and
- real-life QKD system transmitter located in Cambridge and Lexington [b-Bunandar].

In these demonstrations, secret key rates of kilobits per second (kbps) to megabits per second (Mbps) and low quantum bit error rates of 1.0 to 5.4% were obtained and weak laser sources were coupled off-chip. A hybrid integration of Si and III/V active materials thus, promises fully integrated QKD transmitter chips.

Secreted key rates can be further increased by exploiting multiplexing techniques. Taking wavelength division multiplexing (WDM) as an example, multiple keys can be co-distributed in a single fibre but at different wavelengths. A proof-of-concept demonstration of a WDM QKD system comprising two InP transmitters and a single SiO_xN_y receiver achieved increased key rates by a factor of two, to 1.11 Mbps over a 20 km emulated fibre [b-Thompson]. Another example is an implementation of a multidimensional chip-to-chip QKD system on two Si chips, based on space-division multiplexing in a multicore fibre [b-Ding]. The prepare-and-measure (P&M) protocol was applied for four-dimensional states by the Si transmitter and receiver and a low quantum bit error was achieved.

Practical QKD implementations can be imperfect, leaving loopholes that undermine the security of the system, one significant example is detector side attacks. Measurement device-independent (MDI) QKD was proposed and demonstrated to tackle this vulnerability. Recently, two independent studies tested the feasibility of using integrated photonics for MDI-QKD, demonstrating the key part of the protocol, which is the Hong-Ou-Mandel (HOM) interference [b-Semenenko] and [b-Agnesi]. Integrated photonics may provide an ideal platform for multiuser chip-based MDI-QKD networks, in which users only pay for low-cost photonic chips, while the most expensive parts (for example, SNSPDs) can be shared among many users in an untrusted node.

Quantum random number generators (QRNGs) provide a high-entropy high-rate source of trusted random numbers for QKD systems. Integrated QRNGs have been demonstrated based on various nondeterministic quantum processes, such as phase fluctuation, vacuum fluctuation, and non-locality. For example, fully integrated QRNGs have been demonstrated in InP chips [b-Abellan] and [b-Roger], in which random numbers were generated from the random phase fluctuations of two-laser interference to achieve Gbps operations. Moreover, quantum theory allows a stronger form of certified randomness, that is, device-independent (DI) QRNG. By violating the Bell inequalities for multidimensional entangled states in a Si chip, randomness was certified in the fully device-independent scenario [b-Wang-2]. It can be expected that, photonic chips can provide compact, robust, fast, and low-cost solutions for QRNGs.

IQP has rapidly evolved to become a versatile platform in the past decade. Although many components and methods to achieve a high level of integration in quantum photonic circuits have been developed, substantial effort is required to move from the single-/few-component level shown thus far to completely functional modules and systems. It can be anticipated that in the next decade, very-large-scale integrated photonics devices and systems will be developed to enable new and revolutionary applications in quantum communications with many photons [b-Wang-1]. QKD systems may benefit from technology combination including silicon-based quantum state encoding chip, silicon-based quantum state active decoding chip with laser and single-photon avalanche photodiodes (SPAD) coupled from off chip, as well as InP QKD transmitter chip, silicon nitride or silicon oxynitride based quantum state passive decoding chip with SPAD coupled off chip.

5.1.2 Satellite-based QKD

QKD uses individual light quanta in quantum superposition states to generate symmetric keys between distant parties with information theoretic security (ITS). In practice, the transmission distance for QKD systems in fibre or terrestrial free space has been limited to a few hundred kilometres due to channel loss and exponentially reduced photon rate. The protocols on which QKD is based are suited to be applied in satellite communications because of negligible photon loss and decoherence in the empty outer space.

In the past two decades, many terrestrial free space and satellite-ground quantum communication related experiments have conducted pioneering explorations for satellite-based QKD:

- the University of Vienna in Austria experimentally demonstrated entanglement-based QKD over 144 km between two islands [b-Ursin];
- the experiment at the Matera Laser Ranging Observatory (MLRO) in Italy demonstrated that the exchange of single photons is achievable between a low earth orbit (LEO) satellite and the ground [b-Villoresi]; and
- the University of Science and Technology of China (USTC) in China reported free space implementation of quantum teleportation over 16 km and verified the feasibility of satellite-based quantum communication [b-Jin].

The realization of a satellite for QKD was kept on hold in Europe and USA but was observed at the beginning of this decade to be a concrete interest in Asia [b-Pirandola-1]. The LEO satellite, Micius, was launched in August 2016 and provided experimental verification of space-to-ground quantum communication protocols including QKD. USTC, China reported decoy-state QKD with several kbps key rate from the satellite to ground over a distance up to 1200 km [b-Liao-1]. QKD was also demonstrated in the downlink from the Tiangong-2 Space Lab with a 57.9 kg QKD transmitter payload to achieve key rate over 100 bps with distance up to 719 km [b-Liao-2]. The National Institute of Information and Communications Technology (NICT) in Japan reported quantum-limited communication experiment based on a small optical transponder (SOTA) lasercom terminal between a microsatellite (48 kg, 50 cm cube) in LEO and a ground station [b-Takenaka]. The perspective of using very compact payloads as nano-sat or cube-sat for satellite-based QKD has become more attractive and spurred the development of space components of great efficiency and small dimension [b-Oi]. In 2015, nanosatellites with quantum light source payloads were launched by the National University of Singapore [b-Tang-1] and 2019 [b-Villar] and are currently being further developed into nanosatellite-to-ground QKD missions. Such a direction is expected to be beneficial for fibre-based QKD as well, for the realization of high performance, power-saving, and compact components, which could be used in QKD systems.

For QKD networking aspects, a satellite could play the role of a trusted node to connect very distant parties and deliver keys to them. Key exchange between the satellite and two ground stations may then be used to generate a secure key between the two terminals via one-time pad (OTP). For example, the Micius satellite was used to demonstrate intercontinental QKD for text and video encryption between the ground stations of China and Austria over 7600 km [b-Liao-3]. Furthermore, satellites could play the role of an entanglement source to provide quantum entanglement distribution to two distant ground stations and enable their entanglement-based QKD and secure cryptography. For example, the Micius satellite was reported to distribute entangled photon pairs to ground stations separated by 1120 km to perform BBM92 protocol QKD and realize 0.12 bps key rate [b-Yin-1]. Beyond QKD, satellites could also perform space-to-ground quantum teleportation and time transfer [b-Yin-2] and [b-Dai].

One of the practical limitations of LEO satellites such as Micius was the fact that the passage over a ground station, referred to as a working window, was limited to just a few minutes per orbit and the relative speed to ground up to 7 km/s. A high-bandwidth and high-precision acquiring, pointing and tracking (APT) system was required to establish a stable space-to-ground link. Geostationary orbit (GEO) satellites, located at 35,786 km above the Earth's equator may be a solution to this limitation because higher orbits could extend the link and working window duration. Quantum-limited coherent measurements of optical signals from a GEO satellite to a ground station was reported by the Max Planck Institute in [b-Günthner]. However, GEO satellites would involve larger losses and the payloads would be exposed to much more aggressive ionizing radiation from the sun.

Experimental investigations of space QKD were mainly carried out during night-time to avoid background radiation noise from the sun, which was another practical limitation of the satellite based QKD application. Full-time operation in daylight is important for the expansion of satellite usage and the possibility of daylight use in intersatellite quantum communication was investigated by USTC, China [b-Liao-4]. Based on precise pointing, a narrow field-of-view, precise temporal synchronization and an up-conversion detector working at 1550nm, the feasibility of daylight operation was verified on the ground.

From the perspective of academia and based on the previously mentioned exploration progress, with more LEO and GEO satellites launched, the satellite-constellation-based global quantum network, as shown in Figure 2, could be expected in the future [b-Liao-4], [b-Vergoossen]. Current progress on satellite-based quantum communication and QKD exploration is, however, mainly focused on academic research to verify the quantum mechanism and experimental phenomena.

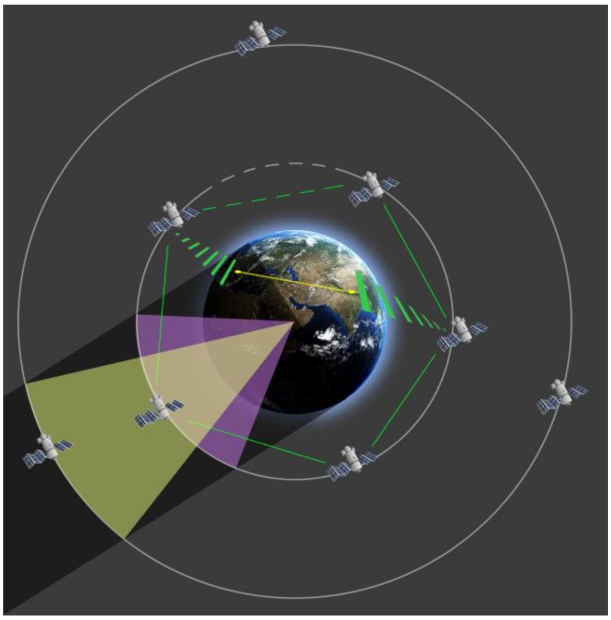


Figure 2 – An expected satellite-constellation-based global quantum network in the future [b-Liao-4]

To achieve a practical satellite-constellation-based global quantum network in future, there could still be a long way to go as aspects such as practical limitations and bottlenecks will need to be overcome. Implementation, networking and application of solutions will require further investigation and the socioeconomic benefits and enablers needed to establish such a constellation will also need to be discussed.

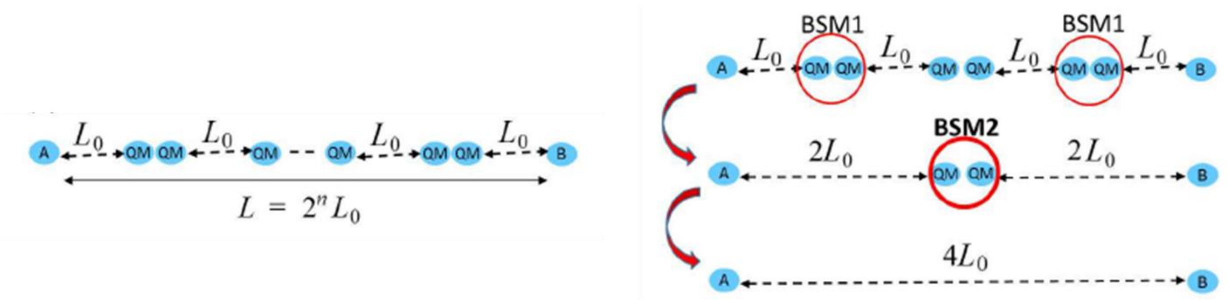
5.1.3 Quantum repeater

To overcome the fundamental rate-loss scaling of fibre-based QKD, multi-hop networks with the assistance of quantum repeaters or quantum relays are needed. Quantum repeaters enable the creation of a known maximally entangled state between the end points of the network by first segmenting the network into pieces, creating entanglement between the segments, and then, connecting those entanglement to create the required long-range entanglement. In a quantum repeater protocol, there are three primary operations required to create the long-range Bell state that can be used for quantum communication tasks such as QKD or teleportation [b-Munro-1]. These operations are:

- **Entanglement distribution:** the process for creating entangled links between network nodes;
- **Entanglement purification:** the process where a more highly entangled state is created from a number of lower quality ones; and
- **Entanglement swapping:** the process in which a Bell-state measurement (BSM) is performed within a node on two qubits which are halves of separate Bell states. The Bell measurement enables a longer entangled link connecting adjacent repeater nodes to be established.

The quantum repeater link procedure, as elaborated in [b-Pirandola-1], presumes that a Bell state has been distributed and stored between two nodes, A and B, at distance L_0 in a network, as illustrated in Figure 3. It is also presumed that node B shares a Bell state with node C farther apart by L_0. Thus, the systems in nodes A and C can be entangled by performing a BSM on the two subsystems in node B.

Principally, to distribute the entanglement over distance L, the entire distance is divided into 2^n segments. The entanglement is distributed and stored over the elementary links with distance L_0 and then BSMs are applied to the middle nodes to extend the entanglement over distance L. This procedure is illustrated in Figure 3.



(a) n nesting levels

(b) 2 nesting levels

Figure 3 – A quantum repeater link with different nesting levels [b-Pirandola-1]

Practical designs for quantum repeaters can be divided into three classes/generations: probabilistic quantum repeaters, deterministic quantum repeaters and memory-less quantum repeaters [b-Munro-1] and [b-Pirandola-1].

5.1.3.1 Probabilistic quantum repeaters

The original repeater protocol requires distribution, storage, swapping, and distillation of entanglement. Interaction with light is necessary for quantum memory to use photonic systems for both distribution and swapping of entanglement. Photon-based systems are, however, susceptible to loss and could result in probabilistic operations requiring a certain procedure to be repeated until it succeeds. Probabilistic quantum repeaters are those that rely on probabilistic techniques for entanglement distribution and entanglement swapping. This class of repeaters has been at the centre of experimental attention in the past 20 years. Entanglement swapping protocols such as Duan–Lukin–Cirac–Zoller (DLCZ) have been proposed and partly demonstrated in practice [b-Duan].

The BSM operation in probabilistic quantum repeaters is typically done by first converting the state of quantum memories back into photonic states and then using linear optics modules to perform the BSM. Such linear optics modules can, however, be inefficient and face certain limitations in offering a full BSM [b-Calsamiglia]. Probabilistic BSM would result in requiring long coherence time and a low entanglement generation rate for probabilistic repeaters. One possible remedy to these problems is the multiple memory configuration which improves the performance in the probabilistic quantum repeater [b-Saglamyurek].

5.1.3.2 Deterministic quantum repeaters

Generating and distributing truly maximally entangled states is very challenging and, in practice, deviations from the ideal case are often experienced. The challenge with this, however, is that after a certain number of nesting levels, the quality of the resulting entangled states is so low that it may not be of any use to quantum applications. If errors are included in the gates, it would become even more challenging. A solution based on the use of purification or entanglement distillation techniques was developed to help overcome these challenges [b-Briegel].

Original distillation schemes relied on performing CNOT gates on pairs of memories [b-Deutsch] and then measuring one of them. The result would be compared with that of a similar measurement at the other end of the link, and success is dependent on whether the two results are, for instance, matched or not.

Another solution that has been developed is using quantum error correction schemes to distil entanglement [b-Jiang] where quantum gates with error rates in the order of 0.001 to 0.01 or below are used to achieve error resilience. Such error correction can also alleviate some of the errors brought about by memory decoherence while waiting for the results on the success of the initial entanglement distribution.

Using these techniques, quantum repeaters with modestly high key rates can be designed with, however, the main limitation arising from the requirement of entangling elementary links still being probabilistic.

5.1.3.3 Memory-less quantum repeaters

The most advanced protocols for quantum repeaters leave as little as possible to probabilistic schemes [b-Munro-2]. In such schemes, loss-resilient error correction techniques are used to make sure that the quantum information carried by photonic systems can be retrieved at each intermediate node. Although quantum memories are no longer needed for storage purposes, they may still be required for quantum processing, which is why they are called memory-less quantum repeaters.

Recently, there have been several experiments on all-photonic quantum repeaters [b-Li-1] and [b-Hasegawa]. While offering a substantial improvement in the key rate, such memory-less quantum repeaters require a set of demanding properties for their required elements. Particularly, operation errors as low as 10^{-4} to 10^{-3}, large cluster states of photons whose generation may require a series of other advanced technologies (e.g., high-rate efficient single-photon sources) and a large number of intermediate nodes are needed.

In fact, the probabilistic nature of BSM and entanglement distribution and the immaturity of quantum memories make practical quantum repeaters possibly unrealizable in the near future. [b-Xu] also points out that the deployment of a quantum repeater is still beyond the capabilities of current technology. Therefore, quantum repeater based QKDN is too immature to be considered from the perspective of standardization.

Some new proposed QKD protocols such as twin-field (TF) QKD and its variants [b-Lucamarini-1] [b-Yu], which can exploit phase-randomization in the intermediate measurement point to extend the transmission link, could be considered as "effective repeaters". Some proof-of-concept experiments have been reported to beat the performance of point-to-point QKD protocols [b-Minder] and [b-Chen-1]. This type of QKD protocols could work well in a star-type network topology by sharing a single detection system among multiple users which is beyond the current point-to-point QKD quantum layer configuration. However, the evolution of QKDN architecture to the adoption of these new QKD protocols and systems need further investigation.

5.2 Experiments and field trials

QKD has been an active research direction in quantum physics for more than 30 years. Scientists and researchers have carried out numerous laboratory-level demonstrations, testbeds, and field trials with various types of QKD protocols and systems. An overview of the characteristics and performance of these QKD experiments, testbeds and field trials, such as technical schemes, transmission distances, key generation rates, etc., will help to better understand the maturity and practicality level of QKD technology.

5.2.1 QKD experiments

Long transmission distances and high secret key rates are important to realize practical QKD applications. After more than three decades of effort since the first QKD experiment was performed in a laboratory demonstration over 32.5 cm of free space [b-Bennett-1], the transmission distance of QKD has been extended to 7600 km by using satellites [b-Liao-3]. Researchers have also recently pushed the secret key rate of QKD to more than 10 Mbps in about 10 km of fibre [b-Yuan-1].

In [b-Xu], typical QKD experiment results were surveyed for protocols including decoy-state QKD, MDI-QKD, TF-QKD, continuous variable (CV) QKD, and others. Tables 1 to 5 summarize some basic information on these experiments with details such as system protocols, operation rate, encoding scheme, transmission channel, distance or loss, and key rate. The survey and summary of these tables provide a convenient perspective for communities outside academia to have a quick review and intuitive impressions about the development progress and the state-of-the-art on QKD experiments.

Table 1 – List of decoy-state QKD experiments and their performance [b-Xu]

Clock rate	Encoding	Channel	Maximal distance	Key rate (bits/s)	Reference
5 MHz	Phase	Fibre	60 km	422.5	[b-Zhao-1] and [b-Zhao-2]
2.5 MHz	Polarization	Fibre	102 km	8.1	[b-Peng]
2.5 MHz	Phase	Fibre	107 km	14.5	[b-Rosenberg-1]
10 MHz	Polarization	Free space	144 km	12.8[a]	[b-Schmitt]
7.1 MHz	Phase	Fibre	25.3 km	5.5 K	[b-Yuan-2]
1 MHz	Phase	Fibre	123.6 km	1	[b-Yin-3]
0.65 MHz	Phase	Fibre	25 km	0.9	[b-Wang-3][b]
1 GHz	Phase	Fibre	100.8 km	10.1 K	[b-Dixon]
7 MHz	Phase	Fibre network	33 km	3.1 K	[b-Peev]
10 MHz	Phase	Fibre	135 km	0.2	[b-Rosenberg-2]
1.036 GHz	Phase	Fibre	100 km	10.1 K	[b-Yuan-3]
4 MHz	Phase	Fibre network	20 km	1.5 K	[b-Chen-2]
320 MHz	Polarization	Fibre	200 km	15	[b-Liu-1]
320 MHz	Polarization	Fibre network	130 km	0.2 K	[b-Chen-3]
1 GHz	Phase	Fibre network	45 km	304.0 K	[b-Sasaki]
100 MHz	Polarization	Free space	96 km	48	[b-Wang-4]
125 MHz	Phase	Fibre network	19.9 km	43.1 K	[b-Fröhlich-1]
1 GHz	Phase	Fibre	80 km	120.0 K	[b-Lucamarini-2]
1 GHz	Phase	Fibre	240 km[b]	8.4	[b-Fröhlich-2]
100 MHz	Polarization	Free space	1200 km	1.1 K	[b-Liao-1]
1 GHz	Phase	Fibre	2 dB	13.7 M	[b-Yuan-1]
2.5 GHz	Time bin	Fibre	421 km[c]	6.5	[b-Boaron]
a: Asymptotic key rate b: Heralded single-photon source c: Ultra-low-loss fibre					

Table 2 – List of MDI-QKD experiments and their performance [b-Xu]

Clock rate	Encoding	Distance or loss	Maximal distance	Reference
2 MHz	Time bin	81.6 km	0.24[b]	[b-Rubenok][a]
1 MHz	Time bin	50 km	0.12	[b-Liu-2]
1 MHz	Polarization	17 km	1.04b	[b-Ferreira][a]
0.5 MHz	Polarization	10 km	4.7×10^{-3}	[b-Tang-2]
75 MHz	Time bin	200 km	0.02	[b-Tang-3]
75 MHz	Time bin	30 km	16.9	[b-Tang-4]
1 MHz	Time bin	20 km	8.3[b]	[b-Wang-5]
250 MHz	Time bin	60 dB	5×10^{-2}	[b-Valivarthi-1]
10.5 MHz	Phase	4 dB	0.1	[b-Pirandola-2][a]
75 MHz	Time bin	55 km	16.5	[b-Tang-5]

Table 2 – List of MDI-QKD experiments and their performance [b-Xu]

Clock rate	Encoding	Distance or loss	Maximal distance	Reference
75 MHz	Time bin	404 km	3.2×10^{-4}	[b-Yin-4]
10 MHz	Polarization	40 km	10	[b-Tang-6]
1 GHz	Polarization	102 km	4.6 K	[b-Comandar][a]
1 MHz	Time bin	14 dB	0.85	[b-Kaneda][a]
1 MHz	Time bin	20 km	6.3×10^{-3}	[b-Wang-5]
20 MHz	Time bin	80 km	100	[b-Valivarthi-2]
50 MHz	Time bin	160 km	2.6[b]	[b-Liu-3]
75 MHz	Time bin	100 km	14.5	[b-Liu-4]
1.25 GHz	Polarization	20.4 dB	6.2 K	[b-Wei]
2 MHz	Time bin	81.6 km	0.24[b]	[b-Rubenok][a]
a: No random modulations. b: Asymptotic key rate.				

Table 3 – List of TF-QKD experiments [b-Xu]

Distance or loss	Key rate (bits/s)	Year	Reference
90.8 dB	0.045 [a]	2019	[b-Minder]
300 km	2.01 K [a]	2019	[b-Wang-6]
300 km	39.2	2019	[b-Liu-5]
55.1 dB	25.6 [a]	2019	[b-Zhong-1]
502 km[b]	0.118	2019	[b-Fang]
509 km[b]	0.269	2019	[b-Chen-1]
a: Asymptotic key rate. b: Ultra-low-loss fibre.			

Table 4 – List of some recent CV-QKD experiments and their performance [b-Xu]

Clock rate	Notes	Distance or loss	Key rate (bits/s)	Reference
1 MHz	Full implementation	80.5 km	~250	[b-Jouguet]
25 MHz	Local LO	——	——	[b-Qi-1]
250 kHz	Local LO	——	——	[b-Soh]
100 MHz	Local LO	25 km	100 K	[b-Huang-1]
10.5 MHz	CV MDI-QKD	4 dB	0.1	[b-Pirandola-2]
50 MHz	High key rate	25 km	~1 M	[b-Huang-2]
1 MHz	Coexistence with classical	75 km	490	[b-Kumar]
5 MHz	Long distance	202.8 km[a]	6.2	[b-Zhang]
a: Ultra-low-loss fibre.				

Table 5 – List of recent experiments of other QKD protocols [b-Xu]

Clock rate	Distance or loss	Key rate (bits/s)	Reference
125 MHz	19.9 km	259	Quantum access network [b-Fröhlich-1]
10 MHz	50 km	–	Centric network [b-Hughes]
500 MHz	53 km	~118.0	RRDPS ([b-Guan]
2 GHz	20 km	2.0 K	RRDPS [b-Takesue]
1 GHz	90 km	~800	RRDPS [b-Wang-7]
10 kHz	18 dB	15.5	RRDPS [b-Li-2]
8.3 MHz	–	456	High dimension [b-Lee]
CW	20 km	2.7 M	High dimension [b-Zhong-2]
4 kHz	–	6.5	High dimension [b-Mirhosseini]
–	0.3 km	~30 K	High dimension [b-Sit]
2.5 GHz	16.6 dB	1.07 M	High-dimension [b-Islam]
625 MHz	307 km	3.2	Coherent one way [b-Korzh]
1 GHz	40 dB	~10	Modulator free [b-Yuan]

5.2.2 QKD field trials

The European Commission Joint Research Centre's (JRC) reviewed QKD field trials and deployments worldwide, including both terrestrial and satellite deployments, as well as publicly funded and privately funded initiatives [b-Martino]. QKD field trials and deployments from four continents and thirteen countries were surveyed and the important progress of the surveyed countries was summarized.

The largest single network is, at the time of this report's publication, in China with a 2000 km long backbone from Shanghai to Beijing and metropolitan networks in these cities as well as in Heifei and Jinan. Smaller deployments have also been made in Korea, Rep. of and in Japan, specifically in Tokyo. Although both China and Japan have experimented with QKD in LEO satellites, the Chinese and Japanese approaches reveal different priorities. For instance, a large network has been built very quickly with technology that is currently available in China, whereas in Japan, work has focused on systematically evaluating the developing technology variants against use cases.

In the European Union, a landmark exercise in QKD field testing was conducted in the FP6 project SECoQC in 2008, in which 6 separate systems were deployed over a three-day period in Vienna. This work was of great importance as it demonstrated the interoperability of different types of QKD systems in a trusted node network. With a network now extending almost the entire length of the peninsula from Turin to Milan and Matera, Italy is home to the largest fibre deployment in Europe. This network is mostly based on commercial equipment and dark fibre (DF), with some university-built hardware in a metro network in Florence. QKD experiments have only been done in some parts of the network and efforts to foster some take-up by prospective users are underway. The SwissQuantum project which operated from March 2009 to January 2011 was the first long term network both in Europe and worldwide. The network included key management and application layers, as well as the quantum layer itself and focused on performance, flexibility, and reliability.

In Spain, the Universidad Politécnica de Madrid together with Telefónica, a major telecommunication operator in the country, built several network prototypes since 2009 [b-Lancho] where research on quantum protocols and its integration within standard optical communication networks have been carried out. In 2018, they built the first QKDN based on SDN deployed in production facilities [b-Aguado]. The current iteration of the Madrid quantum communication infrastructure (MadQCI, 2021）is focused on the integration of QKD technology into real production networks. The network is deployed over the facilities of Telefonica and RediMadrid, a network provider of all research and educational centres in Madrid. In both cases, quantum and classical communications share the infrastructure on a real environment under extremely strict service level agreements. A border node manages and orchestrates both networks such that any node can connect with any other, without restrictions. The network is highly heterogeneous, and in November 2021, comprised of 22 QKD devices (emitters and receivers) from 3 different vendors, combining O-Band and C-Band Systems and discrete and continuous variable systems. QKD systems are combined with 4 Level-1 and 8 Level-2 hardware encryptors. All the quantum infrastructure is seamlessly integrated with classical off-the-shelf optical transport equipment, OADM modules, programmable switches, etc. Standard protocols and tools, well known by telecommunication operators and highly based on public standards from ETSI, ISO and ITU as well as RFCs from IETF, are used throughout. There are 12 different use cases running in parallel over the network in a constant way. These use cases cover a broad spectrum of real communication on networks, from business-to-business services, for example, industrial traffic over 5G, critical and network infrastructure protection, data-plane encryption, etc. There are also several research tasks being undertaken that are analysing from lower optical levels to upper layers of service operationalization of QKD services on real networks.

In the Russian Federation, test networks have been deployed in Moscow, where the work has mainly focused on applications, especially in the banking sector and in St. Petersburg where a testbed has been used to test a novel high-speed protocol.

In the United Kingdom, metropolitan networks in Cambridge and Bristol are currently operational and the link from Cambridge to London is under test. The Cambridge local area network extends to near Ipswich and has been used, notably, with Toshiba's multiplexed equipment in high-speed quantum channel demonstrations. The metropolitan network in Bristol is being used to deploy QKD in a 5G network, again with QKD used along with SDN. A network is also currently under construction in the United Kingdom which will incorporate both long distance and telecommunication network integration.

In the United States, fibre-based and free-space experiments were made as early as 2004 in the Boston area. Relatively little activity took place subsequently in the United States until the private Battelle organization deployed a system in Ohio in 2013. In 2019, Quantum Xchange began a project to link the New York financial centre to data centres in New Jersey, with ambitious plans for a Boston to Washington link. The United States has recently launched a national quantum program within which the National Aeronautics and Space Administration (NASA) has published a vision and roadmap for quantum activities in space.

In Canada, ground deployments have been tested in Calgary and preparations are well advanced for a satellite mission. It will build on the Institute of Quantum Computing's 2016 demonstration of a quantum uplink to an aircraft.

In 2009, a test network with four nodes was deployed in Durban, South Africa, the longest link being 27 km, using commercial equipment in DF.

The secure key rate of QKD in the field deployments depended on the link distances and losses, protocol, hardware and whether DF was used. [b-Martino] provides some basic information on the previously summarized field-trials and deployments in different countries, as illustrated in Table 6, focusing on the distances and secure key rates as the parameters of most importance to potential users. Field trial results from KT Corp. are also provided in Table 6.

NOTE – The results from KT Corp. in Table 6 are not included in [b-Martino] but were provided by in a separate contribution to FG-QIT4N.

Table 6 – QKD field deployments using optical fibre with P&M protocols

Deployment	Span length (km)	Span loss (dB)	Channel	Method	Secure key rate (kbps)
Battelle Ohio	25	19	DF	DV	~1
BBN-Harvard	10.2	5.1	DF	DV	1
Calgary	18.6	9	DF	MDI	0.001
Cambridge metro	5.0/9.65/10.4	1.2/3.3/3.4	DF/LF	DV	3200~2900/3200~2700/ 2500~1400
Cambridge-Duxford	66	16	LF	DV	80
Cambridge-Telehouse	120	29	DF	DV	2
Durban	2.6	——	DF	DV	0.9
Florence	40	21	DF	DV	3.4
Hefei	17/25/30	5.1/9.2/8.1	DF	MDI	0.0388/0.0291/0.0165
Hefei metro	Several, 0.9 to 16.9	0.6 to 6.1	DF	DV	16 to 1
Hefei-Chaohu-Wuhu	85.1/69.7	18.4/14.1	DF	DV	0.77/0.8
IDQ in Japan	13	11	DF	DV	0.3
KT corp. Gwangju to Gonjiam (5G commercial network)	15	6	LF	DV	0.01
KT corp. Bundang IDC to Supreme Court	20.34	8	DF	DV	0.01
KT corp. 1st Digital New Deal national project (2020)	260 (10 nodes)	16 (average)	DF	DV	0.01
KT corp. 2nd Digital New Deal national project (2021)	237 (7 nodes)	15 (average)	DF/LF	DV	0.01
Madrid-backbone (2009)	6	——	LF	DV	0.5
Madrid-GPON (2009)	3.5	——	LF	DV	0.02
MadQCI (Madrid Quantum Communication Infrastructure, 2021)	120.3 (9 nodes, 22 devices)	~0.2 to ~10	DF/LF	DV and CV	~2.780-20.121 depending on the link
Micius	LEO, 500-1200	~28 to ~33	Space	DV	1.1 (~300kb per pass)
Mitsubishi	24	13	DF	DV	2
Mitsubishi- Gakushin U.	10	7	DF/LF	CV	50/27.2
Moscow	30	13	DF	DV	0.1
NEC-NICT	45	14.5	DF with clock/sync	DV	80
NTT-NICT	90	27	DF	DV	2.1
SECOC: Vienna-AIT-Kista	16	——	DF	EPR	2
SECOQC: CNRS-THALES-ULB	6.2	2.8	DF	CV	8
SECOQC: GAP-IDQ-AIT	82	——	DF	DV	0.6
SECOQC: ID Quantique	25	5.75	DF	DV	1
SECOQC: TREL	33	7.5	DF	DV	3.1
Shanghai academic	Several, 2 to 40	3 to 15	LF	CV	10 to 0.25

Table 6 – QKD field deployments using optical fibre with P&M protocols

Deployment	Span length (km)	Span loss (dB)	Channel	Method	Secure key rate (kbps)
Shanghai-Hefei-Beijing backbone	2000 (32 nodes)	18 (average)	DF	DV	20 to 30
Sicily - Malta	96	22	DF	EPR	~0.06 (predicted)
SK Telecom, Daejeon and Sejong	50	——	DF	DV	10
Swiss Quantum	3.7/14.4/17.1	2.5/4.6/5.3	DF	DV	2.4/0.9/0.9
Tiangong-2	LEO, 388 to 719	~32 to ~42	Space	DV	0.091 (~13kb per pass)
Torino-Santhià	100	30	DF	DV	0.25
Toshiba Tokyo 2015	45	14.5	DF	DV	300
TREL	45	14.5	DF	DV	300
Vienna team in Tokyo	1	1	DF	EPR	0.25
Wuhu metro	Several, 9 to 14.3	5 to 7	DF	DV	6 to 1
Xi'an-Guangzhou	30/50	12.48/11.62	DF	DV	5.91/5.77
Zhucheng to Huangshan (Jinan-Qingdao)	66	~13	LF	DV	~3

Quantum-based techniques for communications security are slowly emerging as a complement to algorithmic and non-quantum physical layer methods [b-Martino]. Use cases where quantum communication technology can provide undisputable advantages have still to be clearly identified – its current drawbacks being limitations of distance and quantum-channel bit rate, the need for specialist infrastructure as well as the difficulty of achieving end-to-end security.

QKD is the most technologically mature application of quantum communications and is already commercially available. However, its uptake has been slowed and relegated to niche cases owing to technical limitations in terms of distance and secure key rate, incompatibility with existing fibre infrastructure and difficulties in achieving the accepted paradigm of end-to-end security [b-Martino].

It is observed that most known deployments have relied on public funding [b-Martino]. A limited number of deployments have received funding from either private entities or potential customers investing to learn about a new technology. Deployments purely based on a private customer's demand for the service to serve immediate essential needs have yet to be identified. Investments made thus far have been motivated by the intention of advancing and acquiring experience in a technology which is thought of as promising; even though its real future role remains unknown.

Despite tangible progress, the lack of well-defined use cases where QKD can provide unquestionable security advantages and the technology gaps that remain limit its adoption for operational purposes.

5.3 Commercial solutions and products

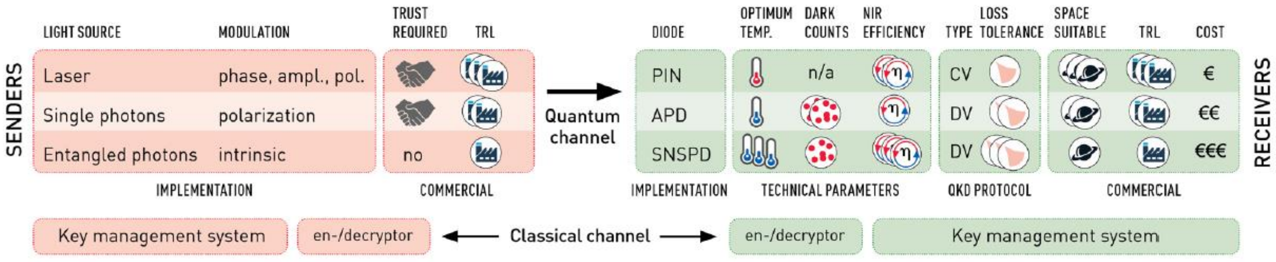
For practical QKDN deployment and application, commercialized products are essential. In the last two decades, commercialized QKD systems, QKD-based encryptors and passive optical components for QKD networks have been available in the market; some which have been deployed in field trial networks and various application scenarios. A summary and analysis on these commercial products could support the assessment of technical maturity of QKD technology.

5.3.1 QKD systems

Quantum communication leverages the properties of quantum state preparation and measurement as well as intrinsic quantum phenomena to create secure communication. Quantum communication can protect networks against the potential data security threat posed by quantum computing. A quantum computer capable of implementing Shor's algorithm could factor large integers exponentially faster than a classical computer, rendering common asymmetric public key encryption protocols such as RSA ineffective [b-NAS].

While it is likely a decade or more away from a quantum computer being capable of breaking RSA 2048, the information security industry is actively working on new solutions to protect against quantum computing attacks. In the software-based realm of post-quantum cryptography (PQC), quantum-resistant encryption algorithms are being developed and going to be standardized. QKD is a complementary hardware-based approach that is already commercially available and ongoing further development. While solution selection will likely be application-dependent, most cryptography experts agree that a hybrid approach, combining QKD and PQC, will be used in the highest security applications for defence in depth [b-OIDA].

In the QKD market, there are several protocols and hardware approaches for distributing encryption keys, including prepare-and-measure QKD, which can be further divided into discrete variable (DV) QKD, continuous variable (CV) QKD, and entanglement-based QKD. The features of these three categories of QKD systems are illustrated in Figure 4 [b-Khan].



TRL= Technology Readiness Level. NIR= near infrared. A larger number of symbols indicates a higher value for the discussed parameter.

Figure 4 – Comparison of DV-QKD, CV-QKD and entanglement-based QKD system [b-Khan]

Quantum state modulation using a single photon source is ideal for QKD systems, however, the single photon source is very difficult to implement. In practical QKD systems, weak coherent pulsed sources combined with polarization or phase modulation are often used as an alternative, combined with decoy state intensity modulation, which has minor impact on the protocol's key distribution efficiency and maintains a physically provable security paradigm. Both single-photon sources and weak coherent laser pulse schemes assume that the QKD receiver inherently trusts the QKD transmitter. The only sources that do not require this trust are the least developed: entangled photon pairs sources that rely on pairs of differently polarised photons generated by a non-linear medium. The non-linear process assigns inherent randomness to the generation of these pairs.

Quantum state light signals can be detected with single photon detectors (SPDs) or homodyne detectors. Practical SPDs include avalanche photodiodes (APDs) and superconducting nanowire single photon detectors (SNSPDs), where APD modules require thermoelectric cooling and have a quantum efficiency of about 20% and SNSPDs require liquid helium cryogenics and can achieve quantum efficiencies of about 80%. Homodyne detection uses a PIN diode-based balanced detector that can be operated at room temperature with quantum efficiencies of 50% to 99%. The tolerable transmission loss depends on the protocol chosen.

Currently, DV protocols can tolerate higher transmission losses than CV protocols. PIN diodes have good characteristics for use in space, whereas APDs have increased dark counts due to radiation and the liquid helium cryogenic environment requirements of SNSPDs make their use in space very challenging.

5.3.1.1 DV-QKD

For DV-QKD schemes, Alice needs to figure out an efficient method to encode qubits in photon or quantum states. Accordingly, Bob needs to develop an efficient method to read the quantum information encoded by Alice. Quantum information can be encoded in two quantum modes and their relative phases. One widely applied method is polarization encoding which utilizes the polarization modes including horizontal and vertical polarizations of a photon, as well as left- and right-handed circular polarizations. Another common method is time-bin phase encoding where Alice chooses two pulses, a signal pulse and a reference pulse, for two encoding modes denoting the photons with a relative phase 0, π, π/2, and 3π/2 between the signal and reference pulses, respectively [b-Xu].

DV-QKD systems, especially those based on the BB84 protocol and its variants, have been commercialized by multiple vendors around the world for over ten years. For further information on the components, interfaces, and requirements of DV-QKD systems, see clause 6.1 of [b-QIT4N D2.4]. However, various quantum state encoding/decoding methods, optical signal modulation/demodulation schemes and distillation post-processing algorithms are used in these commercialized DV-QKD systems, which creates a practical barrier for QKD system interoperability and standardization. Table 7 provides a non-exhaustive list (with products listed in no particular order) illustrating varying technical features and parameters of some current commercial DV-QKD systems from different vendors.

Table 7 – Features of commercial DV-QKD systems from different vendors (Not exhaustive)

Product	Features and parameters
DV-QKD product #1	• Bit-error-ratio (@50 km): <3.5% • Coded scheme: Phase encoding + decoy state BB84 agreement • Maximum communication distance: 100km (@20dB) • Secure key formation rate (@50 km, 1 GHz): >40 kbps • Trigger frequency: 250/500/1000 MHz
DV-QKD product #2	• Maximum transmission loss: 12 dB/14 dB/16 dB/18 dB • Maximum length (typ. @ 0.24 dB/km): 50 km/58 km/66 km/75 km. • Secret key rate: 1.4 kb/s (12 dB) • Key generation rate: 1.25 GHz pulse repetition rate • Key security parameter: $\varepsilon_{\mathrm{QKD}}$= 4.10^{-9}
DV-QKD product #3	• Key rate @25°C: ≥1 kbps @ 24dB • Multiplexing: support quantum channel wavelength division multiplexing WDM • Operation frequency: Max. 1250 MHz • Operation wavelength: 1550.12 nm (default) • Protocol: Polarization-encoded decoy BB84 • Quantum security: against attacks such as photon beam splitting, light blinding, double-click, Trojan horse, laser seeding
DV-QKD product #4	• Detection: Room temperature operation InGaAs detectors • Multiplexing compatibility: CWDM or DWDM with >32×10 Gbit/s channels • Performance: Secure key rate over 1 Mb/s for 10 dB loss Max supported transmission loss >20 dB (equivalent to 100 km of fibre) • QKD Protocol: T12 protocol, a modification of standard BB84 protocol with decoy states, stable encoding onto phase of <50 ps optical pulses • Security parameter: Key failure probability <10^{-10}
DV-QKD product #5	• Bit-error-ratio (@80km): <3.5%

Table 7 – Features of commercial DV-QKD systems from different vendors (Not exhaustive)

Product	Features and parameters
	• Maximum length (typ. @ 0.25 dB/km): 80 km • Secret key rate: 10 b/s (20 dB) • Operation frequency: 1 MHz pulse repetition rate • Operation wavelength: 1550.12 nm (default) • QKD Protocol: BB84 protocol with decoy state
DV-QKD product #6	• Protocol: BB84 protocol with decoy state • Operation frequency: 1 MHz pulse repetition rate • Maximum length (typ. @ 0.26 dB/km): 50km • Secret key rate: 10 bps (@13dB) • QBER: <5% • Operating wavelength: 1550 nm • Random number generation: QRNG

5.3.1.2 CV-QKD

Unlike DV-QKD, the secret keys in CV-QKD are encoded in quadratures of the quantized electromagnetic field and decoded by coherent detections. Coherent detection is a promising candidate for practical quantum cryptographic implementations due to its compatibility with existing telecommunications equipment and high detection efficiencies without the requirement of cooling [b-Weedbrook].

The Gaussian modulated coherent-state (GMCS) protocol is believed to be the core of today's CV-QKD product implementations [b-Grosshans]. Here, the key is encoded in the random phases of coherent states, and the source is an N-discrete randomized coherent-state mixture [b-Ralph]. However, complete security proof of the discrete modulated protocol that gives a good key rate in practice is challenging [b-Xu].

CV-QKD systems also have some prototypes and commercial products from different vendors, however, the commercialization maturity of CV-QKD is currently lower than DV-QKD. For further information on the components, interface, and requirements of CV-QKD systems, see clause 6.2 of [b-QIT4N D2.4]. Its potential application in metro area networks with compact integration and a cost advantage may be attractive for traditional optical communication system vendors to join the game. Table 8 provides a non-exhaustive list (with products listed in no particular order) illustrating varying technical features and parameters of some current commercial CV-QKD systems from different vendors.

Table 8 – Features of commercial CV-QKD systems from different vendors (Not exhaustive)

Product	Features and parameters
CV-QKD product #1	• Detection homodyne detectors, room temperature • Max supported transmission loss: >20 dB, max rate 10 s of kbit/s at max distance • Multiplexing capability in C-band depends on distance and overall intensity of dBm scale channels • QKD Protocol: CV QKD, Gaussian modulation • SDN control capability

Table 8 – Features of commercial CV-QKD systems from different vendors (Not exhaustive)

Product	Features and parameters
	• Switching between many receivers
CV-QKD product #2	• Compatible with DWDM channels: under investigation • Modulation Formats: BPSK, QPSK • Operational wavelength: C-Band (1530-1570 nm) • Symbol rate: 10 GBaud
CV-QKD product #3	• Compatible with current telecommunication technologies and the ability to use standard fibre connections allow for cost effective systems • Free space QKD: can operate unimpaired in daylight conditions, without any filtering • Performance: the use of lasers to encode the signal enables high throughputs • Reduced form-factor: the ability to use COTS components and integrated functionalities allow for reduced form-factor, power, weight, and cost
CV-QKD product #4	• Authenticated key rate: 25 kbps@10 dB, 1 kbps@20 dB • Operation frequency: 10 MHz • Operation wavelength: 1550 nm • Protocol: Gaussian-modulation coherent state GG02 protocol • Transmission distance: <100 km

5.3.1.3 Entanglement-based QKD

For entanglement-based QKD, such as BBM92 protocol, an entangled-photon source via parametric down-conversion (PDC) process is normally adopted. In a PDC process, a high frequency photon is converted to a pair of low frequency photons. A PDC source emits a superposition state of different numbers of photon pairs. In the receiver, single-photon detection is realized with threshold detectors that can distinguish the vacuum (zero photon) from either single-photon or multiphoton cases. Then, Alice and Bob measure the EPR pairs locally by randomly choosing between their bases. Comparing a subset of their measurement results allows Alice and Bob to generate the sifted key [b-Bennett-2].

Due to the difficulties in preparation of high-quality quantum entanglement and Bell state measurement, the current degree of commercialization for entanglement-based QKD is relatively low. There is a view that entanglement-based QKD has not been deployed commercially yet [b-OIDA]. Table 9 provides a non-exhaustive list (with products listed in no particular order) illustrating these varying technical features and parameters of some current commercial entanglement-based QKD systems from multiple vendors.

Table 9 – Features of commercial entanglement-based QKD systems from different vendors (Not exhaustive)

Product	Features and parameters
Entanglement-based QKD product #1	• Entanglement: Polarization • Key Length: 256 bits • Maximum fibre distance: 25 km • Maximum Key Rate: 250 keys/second • Model 1570: Photon wavelength: 1570 nm • Model 810: Photon wavelength: 810 nm • QKD protocol: Bennett-Brassard-Mermin 1992 (BBM92)

Table 9 – Features of commercial entanglement-based QKD systems from different vendors (Not exhaustive)

Product	Features and parameters
	• Quantum state: Entangled Bell singlet state
Entanglement-based QKD product #2	• Detection: Room temperature operation InGaAs detectors. • Operation frequency: N.A. (Continuous) • Maximum communication distance (0.4 dB/km) = 20 km • Secure key generation rate (@20km) = 40 bps @ 8dB • Multiplexing: support quantum channel wavelength division multiplexing (WDM) • Operation wavelength: 1320 nm • Protocol: Polarization-encoded BBM92 • Notable quantum security features include: i. robust against photon number splitting attack without employing decoy states by distributing single (not multi) photon states using entangled photons ii. employment of passive elements for state encoding allows the protocol implementation to be robust against Trojan horse attacks.

5.3.2 Encryptors

Encryptors belong to the encryption application layer device in QKDNs. By using the key generated by QKD combined with symmetric encryption algorithms such as AES-128/256, the information is encrypted in the transmitter and the ciphertext is transmitted through the classical channel. The QKD key from the receiver is then used to decrypt the plaintext. The QKD-based encryptor is similar to the traditional encryptor based on classical cryptography (IPsec, SSL protocols, etc) with the only exception being that the QKD-based encryptor adds new functions of receiving, storing, and encrypting by using the QKD key directly or processed symmetric key derived from the QKD key. The cryptographic key provided by QKD has security advantages over the traditional internet key exchange (IKE) exchanged key from IPsec protocol. Furthermore, the encryption key update rate provided by QKD can also be accelerated to a higher level compared to traditionally exchanged keys which enhance the security level of encryptor.

From the standardization point of view, additional functions such as the QKD key access and storage as well as encryption based on the QKD key could be investigated and standardized to ensure certain security levels. Furthermore, the performance of the QKD key update rate, throughput and delay of an encrypted service based on a QKD key and different encryption algorithm also need to be considered and specified to fulfil the requirement of an encryption application.

QKD-based encryptor products have a variety of prototypes and commercial products provided by different vendors. Table 10 provides a non-exhaustive list (with products listed in no particular order) illustrating varying technical features and parameters of some current commercial QKD-based encryptor systems from different vendors.

Table 10 – Features of commercial QKD-based encryptor system from different vendors (Not exhaustive)

Product	Features and parameters
QKD-based encryptor product #1	• ETSI quantum key interface for interworking with QKD terminals • Encryption of optical transport, Ethernet link/LAN, virtual router interfaces • 100 Mbps to 100 Gbps featuring IP/Ethernet and OTN interfaces • Low latency HW-based line-rate encryption • Hybrid key exchange with Diffie-Hellman and post-quantum key exchange protocols • Security management featuring separation between customer / operator domain
QKD-based encryptor product #2	• 100/1000Base-T interface: 4/6 • Cryptograph throughput: 100/300 Mbps • Delay: 45 μs • Quantum key update: Real-time, configurable • VPN tunnel: 800/3000 pcx
QKD-based encryptor product #3	• Combines security & unparalleled network performance up to 100 Gbps • Compatible with P2P and multi-point architectures • Offers flexibility, extensibility & investment protection for future network growth • Quantum TRNG for high-quality encryption keys (selected encryptors) • Quantum-safe for long-term protection of mission-critical data (selected encryptors)
QKD-based encryptor product #4	• Compatible with QKD key, based on IPSec VPN protocol to improve the security level of transmission link • Integrated routing, switching, firewall, NAT gateway, VPN gateway functions • Separated control and transport design, providing professional firewall function • Support multiple commercial password encryption algorithms
QKD-based encryptor product #5	• fully support mainstream operating systems and mainstream browsers • the key security level can guarantee at least one-time pad • Uses quantum key to realize access authentication and service protection
QKD-based encryptor product #6	• 10Gbps encryptor unit: 1 slot ※ Max 80 slot (800 Gbps) • Algorithm: AES-GCM or ARIA-GCM • Latency: <10 microseconds • Network protocols: 10GbE, 10G OTN (40G/100G Ethernet/OTN planned) • RNG: Quantum random number generator
QKD-based encryptor product #7	• Supports throughput of 10 Gbps (100 Gbps planned) • Layer 2 encryption • Supports point-to-point and point-to-multipoint configurations • Seamless QKD integration via ETSI interface • Upgrade path to implement PQC algorithms • Quantum Side-Channel Analysis (SCA) resistant • Bespoke algorithm customization for high security/assurance applications

Table 10 – Features of commercial QKD-based encryptor system from different vendors (Not exhaustive)

Product	Features and parameters
QKD-based encryptor product #8	• Encryption layer: Layer 1, OTNsec • Client side interface: 1GE, 10GE, 100GE, OTU2/2e, OTU4, STM-1/4/16/64, 1G/2G/4G/8G/10G-FC • Line side interface: OTU2/2e, OTU4 • Encryptor unit: 1 slot (max 88 slot (8.8 Tbps)) • Algorithm: AES-GCM, GCM-SHA256, ARIA-256 • Hybrid key exchange based on QKD and ECDH (Elliptic-Curve Diffie–Hellman) • Latency: <5 microseconds • TRNG: quantum level true random number generator based on QEC (Quantum Entropy Chip)

5.3.3 Passive optical components for QKDN

One of the main challenges of adapting classical communication networks for QKD is the requisite change to the fundamental network infrastructure. This is because QKD technologies have unique features and restrictions, such as the requirement for point-to-point "quantum" channels that are not only ultra-low loss but also ultra-low reflectance. In addition to the higher-level systems and protocols, QKDNs also require a physical layer infrastructure which will allow single or entangled photons to be conveyed from Alice to Bob without decoherence i.e., the collapse of the wavefunction. Decoherence will be caused by direct measurement or by disruption to the photon propagation due to aberrations (imperfections) in the optical channel (optical fibre, connectors, multiplexers, etc.). The chances of transmitting a photon from transmitter to receiver without or with minimal disruption, absorption or decoherence, decreases as the length of the quantum channel increases and the quality of the quantum channel decreases.

Therefore, the emergence of QKDNs and associated systems and protocols will also require a new generation of high performance or specialist passive optical components, which will allow greater probability of the single or entangled photons to propagate over optical networks without decoherence, thus improving the efficiency of the quantum optical network. Given that the power of a single photon can be of the order of −100 dBm, transmission over longer quantum channel distances represents a considerable challenge and thus the optical losses in the quantum channel must be minimized. Table 11 provides a non-exhaustive list (with products listed in no particular order) illustrating varying technical features and parameters of some current commercial physical layer network components for QKDN from different vendors.

Table 11 – Varying features of commercial passive optical components for QKDN from different vendors (Not exhaustive)

Product	Features and parameters
Connector product #1	• Target insertion loss: ≤ 0.05 dB average and ≤ 0.1 dB max. • Target optical return loss: ≥ 80 dB @ 8 ° APC polishing.
Hollow core fibre product #1	• Compatible with existing networks and systems equipment.
Hollow core fibre product #2	• Includes indoor/outdoor cable and termination with standard connectors.
ULL optical fibre product #1	• Maximum attenuation of 0.17 dB/km at 1550 nm.

Table 11 – Varying features of commercial passive optical components for QKDN from different vendors (Not exhaustive)

Product	Features and parameters
ULL optical fibre product #2	• Reduced density fluctuation of a pure-silica core. • Transmission loss of 0.14 dB/km @ 1550 nm.
ULL optical fibre product #3	• Insertion loss is as low as < 0.15 dB/km at 1550 nm.

6 Industry status

6.1 Market players

Currently demonstrated QKD applications and network construction have provided initial business opportunities for system vendors and network operators. Several QKD market players have gradually emerged globally to provide commercial QKD technology solutions and encryption application services and these industry advances provide another important piece of evidence of the maturity of QKD technology.

6.1.1 System vendors

In the innovative technology market, the emergence of multiple QKD system equipment suppliers is not only an important sign of technological maturity, but also an important factor contributing to the need for interoperability and standardization. In the past decade, QKD hardware systems have been commercially available from many suppliers around the world. See Table 12 for a non-exhaustive list of global QKD system vendors summarizing some basic information and their technical solutions.

Various system protocols have been used by system vendors in their QKD systems with the most widely used being the decoy-state BB84 protocol. Commercial QKD systems also use different quantum state coding schemes, often with their own intellectual property rights, which has made interconnection and interoperability of the QKDN quantum layer difficult, if not impossible. From a deployment and application perspective, QKD is a point-to-point quantum state P&M system, the need for interconnection between different vendors at the quantum layer did not appear to be a significant requirement compared to the key transfer and interconnection in the key management layer.

Table 12 – Non-exhaustive list of QKD system vendors

QKD system vendors	Basic information and technical solutions
QKD system vendor #1	• Start-up incubated by a university. • Provider of QKD products with F-M phase coding scheme, point-to-point quantum cryptography communication technology, quantum cryptography communication networking technology, QKD system components.
QKD system vendor #2	• Start-up incubated by a university. • Provider of quantum-safe cryptography solutions, quantum-safe network encryption, commercial QRNG solution, secure quantum key generation, QKD solutions and services as well as optical instrumentation products.
QKD system vendor #3	• Hosted by a research institute. • Provider of QKD systems based on coherent telecommunication technology for metropolitan security applications.

Table 12 – Non-exhaustive list of QKD system vendors

QKD system vendors	Basic information and technical solutions
QKD system vendor #4	• Start-up incubated by a university. • Provider of chip-based QKD solutions.
QKD system vendor #5	• One of the earliest QKD commercial equipment suppliers. • Provider of quantum cryptography solutions that deliver advanced network security.
QKD system vendor #6	• Incubated by a university. • QKD system provider in backbone of "Beijing-Shanghai trunk line" and "Wuhan-Hefei trunk line". • QKD system provider in metropolitan area network such as Hefei, Jinan, Wuhan, Beijing, Shanghai, Guiyang. • Provider of a QSS-ME solution for quantum security mobile communication.
QKD system vendor #7	• Start-up whose solutions utilize entangled photons which are protected by the laws of quantum physics against undetected tampering. • Provider of quantum cryptography solutions for machine-to-machine (M2M) communications and trial testing a quantum cryptography solution that will provide quantum-safe authentication and encryption to automation devices.
QKD system vendor #8	• Provider of solutions for centralized enterprise key and policy management, high-speed true random number generator, an integrated hardware security module, and highly secure encryption for data in uncontrolled environments. • Provider of a quantum cyber-security product that delivers an integrated solution generating, sharing and managing encryption keys.
QKD system vendor #9	• Start-up incubated by a university. • Provider of a quantum communication solution using continuous-variable technology, which realizes the convergence of quantum communication transmission and telecommunication operators' classical communication networks.
QKD system vendor #10	• A member of SMARTS Group of Companies. • QKD system using traditional communication lines. Guaranteed intrusion detection. • Ability to change encryption keys over 10 times per second. Unlimited in time security. • Small-scale production of quantum crypto-gateways.
QKD system vendor #11	• R&D institution. • Provider of a quantum cryptography system to secure optical communications, developed an advanced nanotechnology solution for future quantum information systems.
QKD system vendor #12	• Spin-off from a quantum optics research group at a university that has previously demonstrated detector blinding attacks that compromises the E91 QKD protocol, and free-space BBM92 QKD. • Provider of a quantum communication solution using polarization-entangled photon pairs using the BBM92 protocol. • Other products include e.g., control and measurement instrumentation and quantum random number generators.

Table 12 – Non-exhaustive list of QKD system vendors

QKD system vendors	Basic information and technical solutions
QKD system vendor #13	• Produced from Telco's technology transfer; prototype system using BB84 protocol with decoy state. • Other products include. • Optical transmission equipment (WDM, PTN, POTN), QKD-based encryption transmission devices (Encryptor), and Legacy network encryption devices.
QKD system vendor #14	• Produced from Telco's technology transfer; prototype system using BB84 protocol with decoy state. • Business area. • Optical Transmission System (POTN, PTN, MSPP, WDM) & Access Gateway, LTE- IoT.

As can be seen in Table 12, QKD system vendors are mostly start-ups incubated from universities and academic institutions which is a similar commercialization path that other innovative technologies have taken. However, the R&D institutions of some ICT giants have also actively invested in the development of prototypes and commercial products of QKD systems.

QKD applications that can be expected to be adopted include in corporate networks, healthcare, defence, etc.; however, additional improvements are needed, including increased range, improved key rates, and lower costs/miniaturized hardware. Quantum memories and repeaters will be vital in scaling fibre-based QKD networks. Active stabilization and synchronization of components for the transmitters and receivers (such as laser frequency, polarization, phase of two optical interferometers) is also critical for long-term operation. From a system engineering perspective, further integration and compatibility with existing infrastructure, networks and value chain players is another major hurdle. Although protocols have been developed, additional experimentation and testbeds are required to prove their effectiveness, which will take time [b-OIDA].

QKD system vendors are one of the main driving forces for the development of the QKD industry. In addition, according to the development of the previously mentioned vendors, some have been in establishment for nearly 20 years, it is hard to say that the QKD commercial market has experienced explosive growth in the past decade. Although QKD has the quantum mechanics advantage of improving the long-term security of symmetric encryption applications, some shortcomings such as limitation in key rate and transmission distance, system stability and reliability, cost and integration, and barriers of integrated networking with existing network infrastructure have hindered the large-scale deployment of QKD technology and products. To overcome these barriers, further theory, protocol and engineering innovation and improvement are needed from both academia and industry.

Standardization could play an important role in promoting QKD technology into commercial applications. By specifying the minimum system functions and performance requirements, certifying system security, and standardizing networking and interoperability of systems from different vendors, it can improve the potential users' recognition and acceptance of QKD technology, unify the requirements for network construction and deployment, and reduce the diversity and cost of system.

In recent years, QKD system vendors have noted to be active participants in QKD standardization, in for example, ETSI ISG QKD, ITU-T SG13 and 17, ISO/IEC and ITU-T, as well as China Communications Standards Association (CCSA).

6.1.2 Network providers

In the past decade, various publicly funded experimental and demonstrational QKDNs have been constructed and deployed around the world, see clause 6.2.2. Some of these networks, such as the

Beijing-Shanghai trunk line and Wuhan-Hefei trunk line are now fully operational. There are some additional commercial QKDN deployment plans that have been proposed by various institutions, start-ups and ICT network providers and a non-exhaustive list of QKD network providers is provided in Table 13.

Table 13 – Non exhaustive list of QKD network providers

Network provider	Basic information and network deployment
QKD network provider #1	• Installed the first commercial QKD system in the US., connecting offices in Columbus, Ohio to a production facility in Dublin, Ohio. • The link provides a 1 Gbps link with Layer2 encryption and requires dedicated dark (unlit) fibre. • Access to DF at the production facility and continuing in a ring around the metropolitan area was provided through partnerships secured with other institutions. The network provider built its own fibre link to connect the Columbus offices to this ring providing the continuous DF link needed for the QKDN to function. • Using the Trusted Node, there are plans to further expand the network to connect to offices near Washington, DC. The total distance for this network would be more than 700 km/420 mi.
QKD network provider #2	• The company is the construction and operation subject of the new-generation information infrastructure "National Wide-Area Quantum Secure Communication Network". • Member of ITU-T and CCSA special task force (ST7) on quantum communication and information technology. • In China, QKD is being widely used to ensure long-term security for numerous users in government and the financial and energy industries, including the People's Bank of China, the China Banking Regulatory Commission, and the Industrial and Commercial Bank of China.
QKD network provider #3	• First leg of its operational QKDN runs from Washington, D.C. to New York City and includes key connections to financial markets on Wall Street with back-office operations in New Jersey with plans to extend nationwide (in US). • Popular use-cases include: – Energy: to protect critical infrastructure and provide intrusion detection capabilities. – Federal government and financial services: to secure critical communications. – Manufacturing: to guard 3D printing networks to ensure intellectual property cannot be stolen.
QKD network provider #4	• Launched QKD national test bed with 5 locations in Bun-dang SKT R&D center network and Dae-jeon national R&D center (KISTI) network, in partnership with the Korean government. • Deployed QKD system into its Wi-Fi commercial metro network from Feb of 2016 (100% uptime to date). • Also deployed its QKD system for LTE network with 350,000+ subscribers in Sejong city (uptime is 100% to date). • Plans for a separate long-haul network to deploy differentiated services based on quantum cryptography under consideration.
QKD network provider #5	• Developing satellite QKD services for encryption of long-distance links and links between distant fibre QKD networks.

Table 13 – Non exhaustive list of QKD network providers

Network provider	Basic information and network deployment
	• Building on heritage of SpooQy-1 CubeSat mission which is demonstrating production of entangled photons in an orbiting nanosatellite. • Systems integrator for fibre QKD solutions, also providing workshops, consultancy and bespoke hardware.
QKD network provider #6	• Self-developed prototype of QKD-related systems and the technologies in 2020. Some technologies and products (KMS, NMS, etc.) are mostly ITU-T Y.38xx series-based. • Deployed and operated QKD networks on various areas; Governments, Factories, Medical canters, IDCs, 5G network, etc. Some iconic applications are Quantum-Drone for social safety, Quantum-Robot for smart factory environment, Quantum-DB for data centers, Quantum-Communication for secure mVoIP, etc.

According to the above QKDN providers' status, there might be two different modes of QKDN deployment and operation:

1) **the operator establishes an independent QKDN:** This will provide encryption key services to various users in the local or wide area, so that they can implement secure encryption of the business. The independent network construction mode still has some challenges in terms of fibre channel resource requirements, infrastructure investment requirements, and key or security encryption business model.

2) **to integrate with the existing ICT network:** ICT network providers integrate QKD systems in their networks and provide on-demand QKD-based channel or service encryption services for government and enterprise private network or data centres. The converged network construction model relies on the infrastructure resources and operation services of ICT network operators to provide QKD-based encryption services as value-added services for security enhancement. The level of integration of QKD systems, fusion with existing networks, and their own costs will be the main issues need to be solved when carrying out such network deployment and promotion.

QKDN providers also actively participate in QKD-related standardization work in SDOs. For example, CAS Quantum Network, as well as SK Telecom and KT Corporation promote standardization of QKDN architecture, functional requirements, and other projects in ITU-T SG13 and SG17.

6.2 QKD relevant activities

Quantum information science and technology will play an important role in the evolution of ICT network technology and industrial transformation. In recent years, many countries around the world have initiated scientific research projects and industry promotion plans on quantum technology. As a branch in the field of quantum information science and technology, QKD, which has entered practical application, has also received attention in quantum-related research projects and investments in various countries. A non-exhaustive compilation of various global scientific research projects, investment plans and activities related to QKD research, application, and industry in different countries and regions is provided in the following paragraphs (in no particular order).

QKD research began in the United States in the early 2000s and was continued throughout the decade by various US government agencies including DARPA, NIST, Sandia Labs, Los Alamos, the US Air Force, and the Department of Energy, as well as private organizations including Battelle and MagiQ, and more recently Verizon, AT&T, Qubitekk, and Quantum Xchange. Early work at the National

Institute of Standards and Technology (NIST) set world records for speed by demonstrating user key transmission of over 1 Mbps using QKD. BBN integrated QKD into a demonstration network, and in 2013, Battelle completed the installation of a commercial QKD-protected network spanning 28 km [b-Battelle]. In 2019, Quantum Xchange (a startup) announced a project to link New York's financial centre to data centres in New Jersey, coupled with an even more ambitious plan for an 800 km, Boston to Washington link [b-QXchange-1], [b-QXchange-2] and [b-Whittaker]. In early 2020, NASA began a public process of developing a roadmap to quantum communications in space [b-NASA] and [b-NRC].

As shown in [b-Teh] and [b-Ben], Canada has been promoting research and development of quantum communication technology since the early 2000s. These research projects cover various aspects of quantum communication, including demonstration of ground- and space-based QKD systems. Some of the recent research projects include:

- development and practical demonstration of MDI-QKD network [b-Qi-2] and [b-Mitacs];
- nano quantum encryption satellite (NanoQEY), a 16 kg nanosatellite to test high-risk technologies, due for launch in 2020/21;
- quantum encryption and science satellite (QEYSSat), a 60 kg satellite with a fully functioning down-link QKD payload [b-Csa];
- quantum memory and repeater [b-Sharman];
- security verification of practical QKD systems.

According to [b-Chen-4], some quantum and QKD related research and industry projects and plans have been initiated by China as follows:

- medium and long-term plans for major national science and technology infrastructure technology infrastructure;
- national medium and long-term science and technology development plan outline;
- outline of the national strategy for innovation-driven development;
- national plan for scientific and technological innovation;
- national development plan for strategic emerging industries strategic emerging industries;
- national technical innovation project planning;
- national special program for basic research;
- the twelfth five-year plan of the national major scientific research plan for quantum regulation research; and
- notice on organizing and implementing the 2018 new new-generation information infrastructure construction project, including the national wide-area quantum secure communication network.

In [b-Guo], two state grid proposed QKD-related projects in China include:

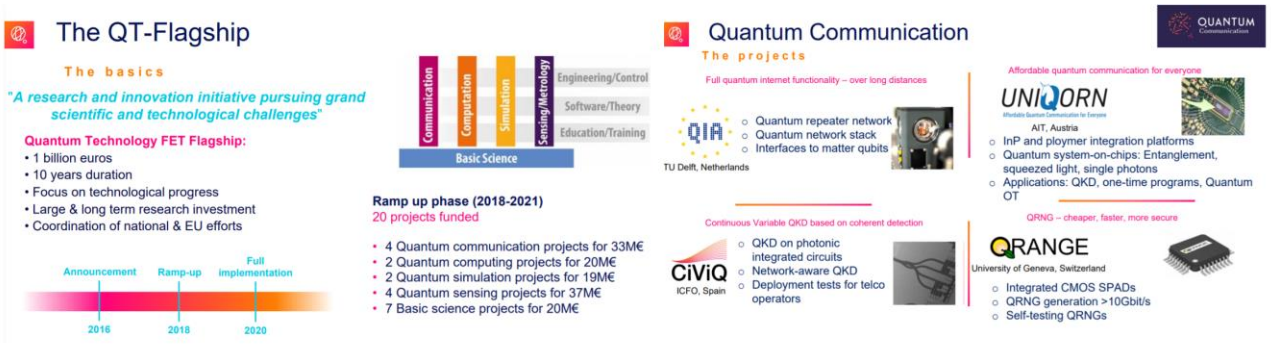
- Project 1: Research on the technology of quantum key anti-interference transmission in power communication (Beijing science and technology commission) was carried out as well as scientific research on rapid bias feedback and networking mode;
- Project 2: Research on the practical application of quantum secure communication in power communication (state grid) was carried out with the key focus on practical application.

Either supported by public research funding or by government investment, QKD-based quantum secure communication demonstrational and trial networks have been built in several cities in China with some long-distance backbone trunks [b-Zhao-3], including:

- 2004: Beijing-Tianjin 125 km, the first quantum cryptography;
- 2007: 4-node Beijing Netcom network of quantum cryptography;

- 2008: Hefei 3-node all-pass quantum secure telephone;
- 2011: Hefei and Wuhu metropolitan quantum secure communication network;
- 2013: Jinan 50-node Quantum Secure Communication Network;
- 2016: Quantum secure communication "Beijing-Shanghai backbone trunk";
- 2017: Quantum secure communication "Nanjing-Suzhou Line", "Shanghai-Hangzhou Line", "Wuhan-Hefei Line", "Jinan-Qingdao Line" and Wuhan Metro Network;
- 2018: First phase of the national wide-area quantum secure communication backbone network.

In 2018, the European Union launched the quantum flagship programme [b-EU-2] with an investment of €1 billion to fund 20 research projects, including four quantum communication projects: quantum internet alliance (QIA) (full quantum internet), UNIQORN (affordable quantum communication), CiViQ (continuous variable QKD based on coherent detection), and QRANGE (cheaper, faster and more secure QRNG).



The QT-Flagship

The basics

"A research and innovation initiative pursuing grand scientific and technological challenges"

Quantum Technology FET Flagship:
- 1 billion euros
- 10 years duration
- Focus on technological progress
- Large & long term research investment
- Coordination of national & EU efforts

Announcement
Ramp-up
Full implementation
2016
2018
2020
Communication
Computation
Simulation
Sensing/Metrology
Engineering/Control
Software/Theory
Education/Training
Basic Science

Ramp up phase (2018-2021)
20 projects funded

- 4 Quantum communication projects for 33M€
- 2 Quantum computing projects for 20M€
- 2 Quantum simulation projects for 19M€
- 4 Quantum sensing projects for 37M€
- 7 Basic science projects for 20M€

Quantum Communication

The projects

Full quantum internet functionality – over long distances

QIA
TU Delft, Netherlands
- Quantum repeater network
- Quantum network stack
- Interfaces to matter qubits

Affordable quantum communication for everyone

UNIQORN
Affordable Quantum Communication for Everyone
AIT, Austria
- InP and ploymer integration platforms
- Quantum system-on-chips: Entanglement, squeezed light, single photons
- Applications: QKD, one-time programs, Quantum OT

Continuous Variable QKD based on coherent detection

CiViQ
ICFO, Spain
- QKD on photonic integrated circuits
- Network-aware QKD
- Deployment tests for telco operators

QRNG – cheaper, faster, more secure

QRANGE
University of Geneva, Switzerland
- Integrated CMOS SPADs
- QRNG generation >10Gbit/s
- Self-testing QRNGs

Figure 5: Quantum communication projects in the Quantum Flagship Programme [b-EU-1]

In 2019, the European project OPENQKD was initiated to test and evaluate QKD equipment against specific use cases [b-EU-4]. OPENQKD will raise awareness of the maturity of QKD and its seamless integration into existing security and networks for a wide range of use-cases.

EuroQCI is an initiative to construct an EU-wide quantum communications network [b-EU-3]. It is envisaged to be certified, secure end-to-end, and composed of space-based and terrestrial-based solutions, enabling information and data to be transmitted and stored ultra-securely and capable of linking critical public communication assets all over the European Union. QKD would be the first service, followed progressively by others as technology becomes available, leading ultimately to the networking of quantum processors at the quantum level.

In 2020, the EU released the strategic research agenda report of the European quantum flagship [b-EU-2], which cites the relative maturity of QKD technology as a motivation to establish testbeds and standards.

In 2020, the Government of India announced the national mission on quantum technology and applications (NMQTA) with a planned funds allocation of > 1 billion USD [b-India]. This mission is expected to cover research and development in all areas of quantum science and technologies including secure quantum communications, quantum computing, quantum sensing and metrology as well as quantum materials.

The Department of Science and Technology of India initiated the quantum enabled science and technology programme [b-QuST] leading to funding of around 50 projects that cover all areas of quantum science and technologies, except quantum materials. Under the above programme, some projects related to different aspects of quantum communications have begun. While some of them relate to the source end of the QKD channel, some are working on indigenous detector technologies and others are aimed at implementing end to end QKD.

One of India's leading quantum communications labs is the quantum information and computing (QuIC) lab at the Raman Research Institute, Bangalore India. Under the India Trento programme for advanced research, an Indo-Italian bilateral programme, the lab is working on integrated photonics-based approaches to QKD. India's first satellite based secure quantum communications project is named quantum experiments with satellite technology. This is also led by the QuIC lab, Bangalore and is a collaboration between RRI and the Indian space research organization. This project started in 2017 and has already achieved several ground-based milestones, including the country's first published work in experimental QKD [b-Chatterjee] and the country's first free space quantum communication experiment through an atmospheric channel using entanglement based QKD between 2 buildings at the RRI campus in early 2021.

In Japan, from 2010, fast QKD systems operating at the GHz-clock were developed and used for successfully demonstrating OTP encrypted video conference in the Tokyo QKD network over a metropolitan area, interconnecting various different types of QKD systems. Since then, long-term reliability tests of QKDN are being extensively investigated in the Tokyo QKDN. As various QKDNs have been operating in realistic field environments, studies on integrating a QKDN into an optical communications infrastructure has started addressing the kinds of security threats that are most likely, how security can be enhanced by introducing a QKDN, and what would be an appropriate architecture for the integration. Research and development on cryptographic applications based on a QKDN is actively underway. Integration methods of a QKDN into the Internet infrastructure have been developed in the form of QKD-secured Layer-2 and Internet protocol (Layer-3) switches. QKDNs enable new applications such as quantum digital signature, and this has been deployed on the Tokyo QKD network.

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

The Tokyo QKD network aims to integrate quantum computing, quantum sensing and quantum cryptography technologies on the network infrastructure and is going to advance into a quantum technology platform with the following steps:

- Stage 1 (2022): QKDN and quantum secure cloud at the Tokyo metropolitan area;
- Stage 2 (2025): Metropolitan QKDNs are formed in Sendai, Tokyo and Osaka, and the QKDNs are connected by satellite quantum cryptography;
- Stage 3 (2030): Enhancement of terrestrial networks and integrated operation of terrestrial-satellite QKDNs.

In [b-Fedorov], the Russian Federation's quantum technologies roadmap is introduced:

- In the field of quantum communications, the Russian Federation's quantum technologies roadmap considers the following directions: point-to-point QKD; trusted-nodes-based QKDNs; untrusted-nodes-based QKDNs; free-space QKD for satellites and drones; quantum-safe (post-quantum) classical cryptography;

- Russian laws require any cryptographic system to be domestically certified if it is used by the government or by commercial entities working on public contracts that require cryptographic information security. Commercial uses of cryptography that do not involve such public contracts are not regulated but nevertheless advised to comply with the same certification procedures. The next phase of the domestic QKD development is standardization and the government body overseeing cryptography has been organizing a series of workshops roughly twice a year to track and coordinate this development with all domestic players and potential users of QKD;
- An important part of the work on standardization is security testing of commercial QKD systems. In this context, it is important to mention that quantum hacking lab is a part of NTI Center for quantum communications at the National University of Science and Technology MISiS.

A two-year R&D call for the development of domestic certification capabilities is upcoming, funded by the National Program Digital Economy.

Quantum technologies in [b-QuantumSG] present research community views and make specific, actionable recommendations from Singapore.

Singapore has been working on quantum communication technologies since the first dedicated quantum laboratory was established in 2002 at National University of Singapore (NUS). Early efforts have built expertise in free-space QKD demonstrating that quantum signals can be distributed in Singapore's urban environment by day and night. Extending this work, Singapore became, in 2016, the first nation to demonstrate a quantum light source in space with the ultimate goal of building global QKDNs via satellite constellations. They have also demonstrated fast QRNGs, a critical device in many cryptographic applications. Steps to commercialize QKD in Singapore are underway with the involvement of network operator Singtel in a corporate laboratory at NUS and the founding of spin-off companies such as SpeQtral and S15 Instruments.

Building on this quantum communications ecosystem, Singapore is in a strong position to compete globally because:

- The country is highly connected and has one of the most advanced optical fibre networks in the world. Tests in the NUS-Singtel Cyber Security R&D Lab have shown that Singapore's fibre network can host sensitive quantum signals. This means fibre-based technology could be deployed quickly;
- Singapore has experts in device and materials engineering who can be engaged to address challenges in quantum communications hardware to build better and more cost-effective systems;
- Singapore is an open country with deep ties to many advanced nations which allows them to collaborate with other countries to co-develop critical support technologies where needed. The S$18 million satellite QKD testbed project established by Singapore and the UK is one such example.

In the near-term (5-7 years), authors of [b-QuantumSG] expect that civil and government entities will begin to deploy QKD systems and to use quantum-enhanced/secure/safe services. On the R&D side, authors of [b-QuantumSG] envisage continued work to build improved QKD and QRNG systems. Looking further ahead, Singapore is in a strong position to build a quantum internet which could secure critical information infrastructures and speed up data analytics. Building a quantum internet would be a highly visible achievement that would increase Singapore's reputation as a safe and reliable city for living and business.

Besides the activities mentioned in [b-QuantumSG], the Quantum Engineering Programme (QEP) [b-QEP] was launched in 2018 by the National Research Foundation, Singapore, and is hosted by NUS. QEP will apply quantum technologies to solve user-defined and application-oriented problems, by funding research and supporting ecosystem building. Its work is focused over four pillars: quantum sensing, quantum communication and security, quantum computing and quantum systems/hardware.

Under the QEP, the National Quantum-Safe Network (NQSN) project hosted by NUS and Fraunhofer Singapore will be initiated in 2022. NQSN will provide a platform for technology exploration, develop a vendor-neutral ecosystem for end-users and stakeholders to demonstrate the integration of quantum-safe applications and will drive testing, certification and accreditation processes for quantum communication solutions and services. NQSN will deploy a quantum-safe communication infrastructure, and advance security evaluation capabilities. In particular, the NQSN will implement a QKDN environment under realistic conditions in which the performance, scalability and security of new and existing quantum security technologies can be studied and explored safely. NQSN will act as the horizontal enabler with additional focus on quantum security to develop core evaluation techniques and countermeasures, in collaboration with governmental agencies and industrial partners e.g., T-system, UL and so on. At the same time, NQSN will serve as a showcase and testbed to end-users, international collaborators and will significantly increase the awareness and facilitate future-ready quantum-safe technologies and solutions, e.g., with ST Engineering and Thales to develop new network encryption solutions with QKD, with Amazon Web Services to boost the development of quantum communication and computing technologies, and to explore potential industry applications of quantum capabilities.

NQSN also intends to be compliant with existing QKDN standards. A task force on the quantum technology standards under IMDA is also planned with its main objectives being to:

1) adopt international standards on quantum technologies to be local technical and reference specifications;

2) share the experience of NQSN and contribute to quantum related standardization works in SDOs such as ITU, ISO, ETSI.

Spain has been working in quantum technologies since the 90s. Its scientific production, as of 2021 is the fourth in the EU, ranked by various papers and the h-index [b-McKinsey]. It has also a large participation in the EU quantum flagship programme as well as in H2020 calls dedicated to quantum technologies (e.g., the OpenQKD project, which is considered the ramp-up project for the EuroQCI and has proposed a satellite with a quantum payload in the framework of the European Space Agency (ESA). Beyond the standard research programs, two additional funding programs have been recently approved in Spain with a total of about €100 million for the next three years (starting 2022). One is dedicated to quantum computing and the other to quantum communications. The quantum communications program is synchronized with the EuroQCI and part of the outcome will be to make the current quantum testbeds (e.g., MadQCI) permanent and also to add more as the national part of the EuroQCI.

In Thailand, the strategic research programme on quantum technology was launched in 2020 by the Ministry of Higher Education, Science, Research, and Innovation [b-NXPO-1]. Quantum research in Thailand is divided into three main pillars: quantum computing and simulation, quantum communication, quantum metrology, and sensing [b-NXPO-2].

For quantum communications, the pilot program involves research groups from all top universities and research institutes across the nation to collaboratively create and demonstrate basic components for quantum-secure communication, namely QKD, QRNG and quantum repeaters. These will be extended into two milestones. The first milestone is to develop Thailand's infrastructure toward quantum-safe communication networks, both ground-to-ground and satellite link [b-GISTDA], domestically and with international collaborators. This also includes developing and implementing PQC protocols as transitioning measures for short-term threats. The second milestone is developing and adopting communication standards and certification protocols for the implementation of quantum-safe cryptography.

In recent years, the development and application of QKD has also attracted the attention of research institutes, regulatory agencies, and other stakeholders globally. A non-exhaustive compilation of various QKD technology evaluations, application recommendations and regulatory opinions can be seen in Table 14. Understanding the current positions of these organizations on QKD technology and applications may be helpful for a comprehensive assessment of QKD technology maturity, application feasibility and industrial development prospects. Specific content on current positions related to QKD, at the time of this report's publication, can be found in the relevant references. The statements referenced in this table represent views from a mix of research, national security, and other governmental organizations.

NOTE – There are various responses and matters of opinions on these public statements available from other organizations and authors.

Table 14 – Sources of public statements on QKD technology (non-exhaustive list)

Title of Publication	Organization	Reference
A roadmap for quantum technologies in the UK	Innovate UK and the Engineering and Physical Sciences Research Council	[b-UK]
Applications of Quantum Technologies	US Department of Defense (DoD)	[b-DoD]
Growing Australia's Quantum Technology Industry	Commonwealth Scientific and Industrial Research Organisation (CSIRO)	[b-CSIRO]
National Agenda for Quantum Technology	Quantum Delta the Nederland (QDNL)	[b-QDNL]
Quantum Key Distribution (QKD) and Quantum Cryptography (QC)	US National Security Agency (NSA)	[b-NSA]
Quantum security technologies. White Paper	UK National Cyber Security Centre (NCSC)	[b-NCSC]
Quantum technologies - from the basics to the market	German Federal Ministry of Education and Research	[b-BMBF]
Should Quantum Key Distribution be Used for Secure Communications?	French National Cybersecurity Agency (ANSSI)	[b-ANSSI]
Strategic research agenda. European Quantum Flagship	European Commission	[b-EU-2]

The above activities and public statements of QKD technology indicate that the application and industrial development of QKD is still evolving and faces challenges.

QKD system performance, security and deployment solutions need further investigation, evaluation, standardization, and certification. Since QKD technology will be used in the field of information security, relevant regulatory agencies and recommendations have already pointed out that standardizing QKD technology and systems as well as carrying out certification to meet certain security requirements are prerequisites for promoting QKD applications. Several SDOs including ITU-T, ISO/IEC and ETSI, have been actively involved in standardization work related to QKD systems and networks and their progress can be seen in Clause 7. Although, different countries will independently adopt their own evaluation and certification schemes to evaluate QKD technology access and deployment, international standardization of QKD systems and networks in terms of protocol, interoperability and security can provide corresponding guidance and technical basis for such evaluation and certification.

Additionally, both QKD and quantum-safe cryptography, also called PQC, may present a possible solution for cybersecurity in the quantum era. QKD and PQC are based on different approaches to deal with information security threats brought on by quantum computing and will also have different costs. Theoretically, QKD has long-term future-proof security; however, there are barriers which need to be overcome related to its performance, robustness, cost, and compatibility. On the other hand, cybersecurity upgrades may be smoother with PQC since the existing public key infrastructure can be leveraged, thus it has advantages in compatibility, cost, application areas, and portability. However, the PQC algorithms currently under consideration may not guarantee long-term security from a theoretical level against future unknown cyberattacks and vulnerabilities. See Appendix I for an introduction to PQC and its standardization status.

The combination of QKD and PQC may enable an optimal solution for future application-specific scenarios with high security requirements, as indicated in [b-Wang-8] and UC-1-3 in [b-QIT4N D2.2]. However, integration details and use-case specific scenarios require further exploration.

From the perspective of driving QKD use cases, strengthening relevant standardization work will play an important role in promoting QKD's evaluation, certification, and large-scale deployment.

6.3 Other aspects

6.3.1 Simulation

QKD systems and networks typically implement physical signal transmission and key generation based on optical fibre networks. The quantum state optical signal is different from the traditional optical communication signal. It is a quasi-single photon level polarization or phase modulated signal with extremely low optical power, or quadratures of the quantized electromagnetic field of the weak coherent optical pulse. The design and analysis of the QKD system in the optical fibre network also have some special features.

Traditional optical communication systems and optical transport networks have mature simulation and design tools and there are companies that have already provided network-level simulation tools based on graphical interfaces, robust simulation schedulers, realistic simulation models and flexible optical signal representations, which can be used for design, test, and optimization of various types of optical fibre communication links.

Suitable simulation and design tools will provide strong support for research on QKD systems and the deployment of QKDNs which will then promote the industrial development of QKD technology. Some strides are being made in this area and this is demonstrated in projects such as the 2019 project supported by the CiviQ of the EU quantum flagship which launched a QKD system simulation toolkit [b-Kreinberg].

In the field of CV-QKD, P&M protocols using weak coherent states are very promising candidates for broad deployment as they use electric field quadratures for encoding the quantum information (QAM). QAM is typical in optical telecommunication and experimental implementations of CV-QKD and implementations using standard telecom hardware have been demonstrated.

Coherent states are often referred to as the "most classical" quantum states and can be understood as electric fields or laser pulses. Consequently, the quadratures q and p of the corresponding quantum field can be described by the real and imaginary part of a complex-valued electric field. For example, typical simulation system treats time-varying electric fields as a time-discrete sequence of phasors relative to a reference frequency. Shot noise occurring during detection of a coherent state using a photodiode can be simulated in this framework by drawing a sample from the corresponding Poissonian distribution. Without further adjustments, it is therefore possible to use the simulation system for simulating P&M weak-coherent CV-QKD systems. The simulation system demonstrated that a classical optical simulation framework can be used for modelling weak-coherent P&M CV-QKD systems and the simulations of various noise sources fit the analytical predictions. The flexibility to selectively turn on and off physical effects and noise sources opens research possibilities which were inaccessible experimentally. Current work focuses on integrating the reconciliation and privacy amplification toolchain into the simulation framework with the goal of providing a comprehensive tool for precise secret key rate prediction.

Typical application scenarios including system design, study of co-existence scenarios, account of component imperfections, and optimization of system parameters are:

- Key functions and modules for CV-QKD system including parameter estimator for Gaussian-modulated CV-QKD, random number generator for Gaussian-modulated CV-QKD, secret fraction estimator for Gaussian-modulated CV-QKD, black box transmitter and receiver, and realistic receiver with automatic shot noise unit (SNU) calibration.
- Key functions and modules for DV-QKD including single photon counting, differential phase shift keying transmitter and receiver, polarization, time/phase and T12 basis BB84 transmitters & receivers, key sifting, random number generator for decoy state BB84, e.g., T12, secret fraction estimator for T12.

A key consideration of simulations related to different aspects of QKD is ensuring that practical aspects of the architecture are properly accounted for. Most simulation tools are focused on the protocol aspects and little attention has been devoted to the details of the imperfections in the attendant optical and electronic components as well as the physical processes. In recent work, researchers have come up with a unique simulation toolkit for end-to-end QKD simulation which is based on modular principles that allow it to be grown to different classes of protocols using various underpinning technologies [b-Chatterjee]. The novelty of this toolkit lies in its comprehensive inclusion of different experimental imperfections, both device-based as well as process-based. Thus, these simulation results are expected to match with actual experimental implementations to a much better accuracy than other existing software, making it a handy and essential tool for QKD experimentalists.

Another simulation toolkit that currently exists in literature and has similar considerations in its conception is described in [b-Mailloux]. While the motivation is similar, its execution is different.

Such simulation toolkits, aimed at bringing in practical imperfections in devices as well as processes into consideration in QKD simulations, are poised to be valuable resources in designing and implementing QKDNs.

The commercialization of QKD systems and network simulation tools can be regarded as a sign of the maturity level of the QKD protocol, system technology and application development. By expanding and improving its simulation and analysis capabilities, it could help to provide effective analysis methods for engineering problems faced in system design and network deployment, thereby improving the efficiency and feasibility of equipment R&D as well as network construction.

6.3.2 Test and evaluation

Testing and evaluation (T&E) is crucial for the marketing and industrial development of emerging technologies. In the case of QKD, potential users would need to know if a QKD system will meet their usability and safety requirements when planning to either purchase a point-to-point QKD system or deploy a QKDN. T&E can, for instance, provide users with verification of a QKD system or QKDN's functionality, performance, and security. It will be an essential link for connecting system vendors and end users to build a complete industrial chain.

T&E, however, also needs the support of standardization. Technical standards could provide specifications on minimum functional, performance and safety requirements for different types of QKD systems in the market. The standardization of test methods could also propose a unified test environment, test steps, and pass/fail criteria to check requirements such as those previously listed. Therefore, carrying out standardization studies on the T&E of QKD systems and networks will be important to promote the development of T&E and further industrial development.

6.3.2.1 QKD system security

Standards about security requirements, test and evaluation methods for QKD systems were under investigation in ISO/IEC JTC 1/SC 27/WG 3 at the time of this report's publication. Its stage documents were provided for comments in [b-Shi].

For security requirements (ISO/IEC 23837 Part 1), its scope includes the specification of a general framework for security evaluation of QKD under the framework of ISO/IEC 15408 (all parts), covering the baseline set of common security requirements on the conventional network components, as well as those on the quantum optical components in QKD modules. Threats that QKD may face in its potential environment are analysed and the security functionality of QKD are identified. For the essence of the network device, the security requirements of QKD modules are mainly characterized under the framework of ISO/IEC 15408 (all parts) and refer the methodology of ISO/IEC 19790 and relevant standards on cryptographic modules testing [b-Shi].

Two types of QKD protocols including DV and CV, three types of QKD architecture such as P&M, MDI and EB were defined and analysed. Security issues and requirements related to the internal and external interfaces and functional components for P&M QKD implementation were also specified.

For test and evaluation methods (ISO/IEC 23837 Part 2), its scope includes the specification of security test and evaluation methods for QKD. Evaluation activities that constitute methods of the security functional requirements on QKD-protocol implementation, quantum optical components as well as conventional network components are specified. Moreover, supplementary evaluation activities for security assurance requirements are specified to support the security evaluation of QKD with appropriate assurance levels.

Specific evaluation activity for a QKD system, transmitter, receiver, and calibration are proposed while a test procedure and judgment criteria were provided. Current test and evaluation use cases in discussion and their purpose are listed in Table 15. Further details can be sourced from ISO/IEC JTC 1/SC 27/WG 3.

Table 15 – Security test and evaluation use cases in ISO/IEC WD1 23837-2 [b-Shi]

Sub-clause	Evaluation activity
6.2	test raw key exchange procedure
6.3	test post-processing procedure
6.4	test calibration procedure
7.2	test the photon-number distribution of the optical pulses
7.3	determine the average intensity and stability of the optical pulses
7.4	test the independence of the optical pulses' intensities
7.5	test the accuracy of the state encoding
7.6	test the independence of the encoded states from wavelength, polarization and arrival time
7.7	test the randomness of the phase of the optical pulses
7.8	determine the level of optical isolation of the transmitter module
7.9	determine the sensitivity of the detector monitoring light injected over the quantum channel
7.1	test the robustness against laser injection
8.2	determine the detection efficiency mismatch in the RX module
8.3	determine that back-flash of QKD receiver does not leak information
8.4	determine the degree of optical isolation of the receiver module
8.5	test the robustness against bright light blinding
8.6	test that the detector dead times are handled appropriately
8.7	determine the area of registering detections for single-photon detectors
8.8	test the robustness against laser injection
8.9	determine the sensitivity of the detector monitoring light injected over the quantum channel

Table 15 – Security test and evaluation use cases in ISO/IEC WD1 23837-2 [b-Shi]

Sub-clause	Evaluation activity
8.1	determine the detection limits of a homodyne detector in a receiver module
8.11	test the correct post-processing of double-click events
9.2	test if detection efficiency mismatch can be aggravated by tampering the calibration procedure
9.3	test the correctness of shot noise calibration

6.3.2.2 QKD system function and performance

Active optical components such as optical sources and single photon detectors are of importance in the security of a QKD system. Specifications and procedures for the characterization of optical components for use in QKD systems has been specified in [b-ETSI GS QKD] providing examples of specific tests and procedures for performing them.

Measurement methods used for the electrical properties, single photon source (QKD transmitter) properties and the single-photon detector (QKD receiver) properties of DV-QKD systems were also specified in [b-ETSI GS QKD], as illustrated in Table 16. Further measurement schemes and procedures can be found in [b-ETSI GS QKD].

Table 16 – Measurement for DV-QKD internal components [b-ETSI GS QKD]

Property	Parameter	Description
Electrical properties	Clock frequency	The frequency of the clock signal
	Clock frequency variation	The variation in the clock frequency over a stated time interval
Single photon source (QKD transmitter) properties	Optical pulse repetition rate	Repetition rate (frequency) of the emitted optical pulses
	Mean photon number	Average number of photons per emitted pulse
	Source power	The average power emitted by the laser over the time period of a QKD session
	Long-term power stability	The variation in source intensity over the duration of a QKD session, or some other stated time-interval
	Short term power stability	The variation in pulse intensity over a set period, e.g. 1 minute
	Source emission temporal profile	The distribution of photons within the emitted pulses as a function of temporal position
	Source timing jitter	The uncertainty in the emission time of a single pulse at the optical output
	Source temporal profile	The intensity variation within a single pulse as a function of temporal position within the optical pulse
	Source wavelength	Wavelength of photons that are emitted
	Spectral line width	Bandwidth of the emitted photons.
Single-photon detector (QKD receiver) properties	Detector gate repetition rate	The repetition rate of the time-intervals during which a detector has single photon sensitivity. In the case of a SPAD, this should correspond to the times during which the reverse-biased p-n junction is biased above the breakdown voltage

Table 16 – Measurement for DV-QKD internal components [b-ETSI GS QKD]

Property	Parameter	Description
	Dark count probability	For a gated detector this is the probability that a detector registers a detection event in a gate of stated duration, in the absence of optical illumination. For a free-running detector this is the probability that a detector registers a detection event in 1 s, or some other stated time-interval, in the absence of optical illumination
	After-pulse probability	The probability that a detector registers a false detection event in the absence of illumination, conditional on a detection event in a preceding detection gate at a time ΔT earlier
	Photon detection probability (Detection efficiency)	The probability that a photon of a specific energy (wavelength) incident at the optical input will be detected within a detection gate
	Linearity factor (for detection efficiency)	Minimum detection efficiency divided by the maximum detection efficiency over the specified range of powers
	Detection efficiency range due to polarization variation of input pulses	The difference between the maximum DE and the DE for randomly polarized light
	Dead time	The time interval after a detection event when the detector as a whole is unable to provide an output in response to incoming photons at the single photon level
	Recovery time	The smallest time duration after which the detection efficiency is independent of previous photon detection history
	Low and high partial recovery times	The time duration after a photon detection event for the detection efficiency to return to x % of its steady state value. x = 5, 10 or some other stated value for tpartial_low; x = 99, 90 or some other stated value for tpartial_high
	Detector signal jitter	Photon detection probability (detection efficiency) variation with respect to the arrival of a single photon at the input port of the DUT
	Photon detection probability (detection efficiency) profile	Photon detection probability (detection efficiency) variation as a function of incident pulse arrival time
	Spectral Responsivity	The photon detection probability (detection efficiency) as a function of wavelength of the incident photons

Some measurement schemes and parameters have also been proposed and conducted for T&E of QKD and QKD-based quantum secure communication systems across multiple vendors in China's market. A test evaluation framework for QKD/QSC system function and performance has also been established and requirements for QSC system and network verification have been considered. Some test and evaluation cases have also been reported in [b-Zhao-3].

The standardization of technology requirements and test methods for decoy-state BB84 protocol DV-QKD system have also been investigated in CCSA-ST7 and the measurement of QKD systems and networks have been conducted in several real-world QKDN deployment scenarios in cities such as Beijing, Shanghai and Jinan [b-Zhao-3].

6.3.3 Certification

Since QKD technology is mainly used in the field of information security, the regulatory requirements for equipment certification and market access might be higher than other technologies used in the ICT field. The scalable deployment of QKD products not only require standardization and T&E but also need to meet more stringent requirements such as different access conditions and certification requirements from different administrations.

Presently, the commercialization and market size of QKD technology, with relatively scattered technical solutions of QKD products, is limited and QKD-related standardization studies are still in the early stages of development. From current publicly accessible information, no specific certification system, access conditions and regulatory requirements for QKD technology or its products have been released. With future developments in the QKD industry, standardization, evaluation, relevant certification, and supervision will also gradually be improved.

7 QKDN standardization landscape

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 Figure 6. The status of QKDN standardization in different SDOs is briefly reviewed in the following sub-clauses.

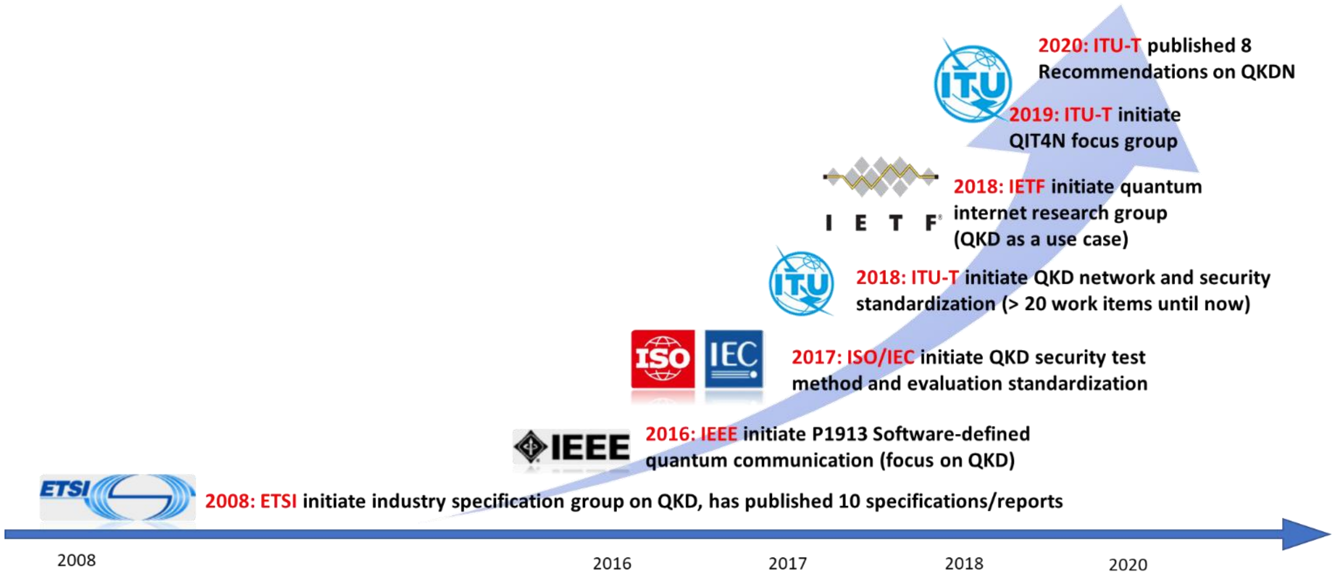

2020: ITU-T published 8 Recommendations on QKDN
2019: ITU-T initiate QIT4N focus group
2018: IETF initiate quantum internet research group (QKD as a use case)
2018: ITU-T initiate QKD network and security standardization (> 20 work items until now)
2017: ISO/IEC initiate QKD security test method and 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 6 – QKDN standardization timeline

7.1 ITU-T

ITU-T was the first SDO to standardize QKD as a network in 2018.

7.1.1 ITU-T Study Group 11

At the time of this report's publication, SG11 had initiated 1 work item on QKDN for study, as listed in Table 17.

Table 17 – 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

7.1.2 ITU-T Study Group 13

At the time of this report's publication, SG13 had adopted 7 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 18.

Table 18 – 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	Quantum key distribution networks - Requirements for quality of service assurance	Recommendation	Published (2021-10)
Q16/13	Y.Sup70	ITU-T Y.3800-series - Quantum key distribution networks - Applications of machine learning	Supplement	Published (2021-09)
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

Table 18 – QKD related work items in ITU-T SG13

Q	Reference	Title	Type	Status
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 distribution networks - Resilience framework	Recommendation	Under 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 7.

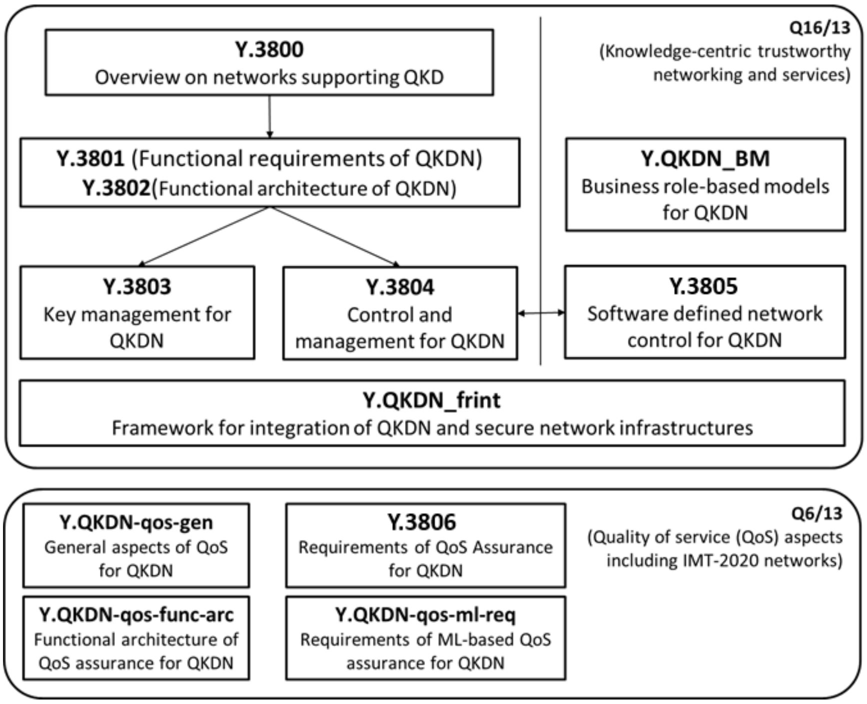

Q16/13
(Knowledge-centric trustworthy networking and services)
Y.3800
Overview on networks supporting QKD
Y.3801 (Functional requirements of QKDN)
Y.3802(Functional architecture of QKDN)
Y.QKDN_BM
Business role-based models for QKDN
Y.3803
Key management for QKDN
Y.3804
Control and management for QKDN
Y.3805
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.3806
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 7 – QKDN standardization work items in SG13

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

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 19.

Table 19 – 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 8.

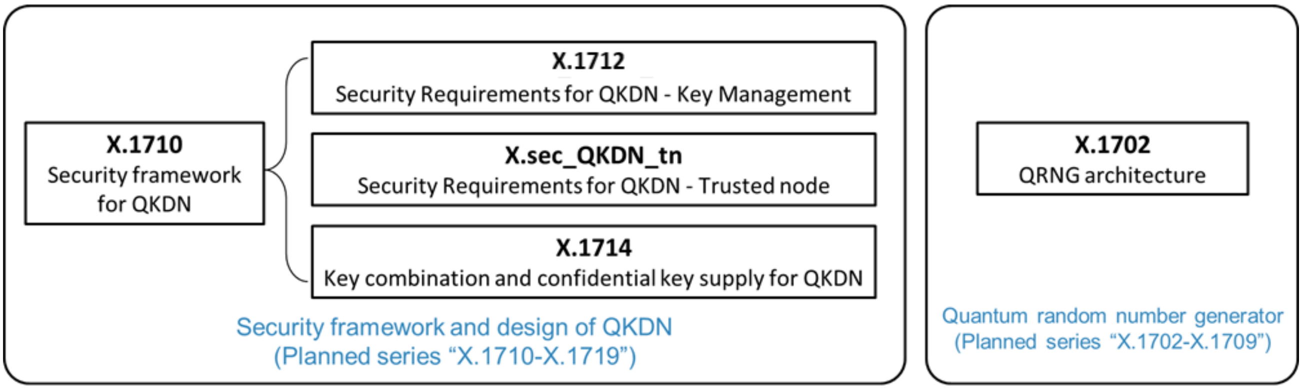

X.1710
Security framework for QKDN
X.1712
Security Requirements for QKDN - Key Management
X.sec_QKDN_tn
Security Requirements for QKDN - Trusted node
X.1714
Key combination and confidential key supply for QKDN
Security framework and design of QKDN
(Planned series "X.1710-X.1719")
X.1702
QRNG architecture
Quantum random number generator
(Planned series "X.1702-X.1709")

Figure 8 – QKDN standardization work items in SG17

7.2 ETSI ISG-QKD

ETSI initiated the industry specification group (ISG) on QKD in 2008. ETSI ISG-QKD had published nine specifications on QKD by 2019 and have several ongoing work items as listed in Table 20. 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 initiated the study of QKDN architectures recently and the specification of QKD security certification based on common criteria.

Table 20 – 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 V1	Quantum Key Distribution (QKD); Application Interface	Published (2010-12)
GS QKD 004 V2	Quantum Key Distribution (QKD); Application Interface	Published (2020-08)
GS QKD 005	Quantum Key Distribution (QKD); Security Proofs NOTE – Revision in progress	Published (2010-12)
GR QKD 007	Quantum Key Distribution (QKD); Vocabulary NOTE – Revision in progress	Published (2018-12)
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 REST-based key delivery API	Published (2019-02)
GS QKD 015	Quantum Key Distribution (QKD); Control Interface for Software Defined Networks Note: Revision in preparation ref. RGS/QKD-015ed2_ContIntSDN	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
DGS/QKD-020_InteropKMS	Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API	Under development
DGR/QKD-019_AUTH	Quantum Key Distribution (QKD); Design of QKD interfaces with Authentication	Under development

7.3 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. The study period was completed in 2019, and a new work item ISO/IEC 23837 (Part 1&2) was established as listed in Table 21.

Table 21 – 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

8 QKDN Standardization outlook

8.1 Gap analysis for QKDN standardization

As observed in Clause 7, although the standardization of QKD begun in 2008, the work related to QKD as a network is still in the beginning stages and the most important standardization issues such as network interoperability and security certification, are still unresolved.

Although the wide-area network coverage and vast applications are key in driving the development of quantum cryptography industry, the QKD network level standards are important and require joint efforts from multiple disciplines including quantum physics, telecom network and information security, etc.

As a new network form which provides key distribution services, QKDNs have both the characteristics of communication networks and cryptographic services. QKDNs are comprised of different communication function modules that are similar to classical communication networks, e.g., signal modulation, transmission, reception, detection and post-processing. Therefore, they need to meet the basic requirements for networks including cost-effective deployment, flexible expansion, interoperability etc. However, services provided by QKDNs are different from classical communication systems, in that random numbers are used for key materials rather than ordered information. Therefore, a QKDN will also need to meet specific requirements for cryptographic services. Considering both the communication network and security service requirements, QKDN, as both a new kind of security tool and a new form of network infrastructure, requires systematic standardization.

Taking the organization of the ITU-T as an example, work on QKDN is already ongoing in SG13 on network aspects and in SG17 on security aspects, see Figure 9. Future work may involve protocols and signalling for network, user, and device interconnection (related to SG11), network operation related specifications for QKDN (related to SG2), integration of QKD with classical optical communication networks (related to SG15) and on QKD applications in data centre interconnection, cloud computing, Internet of Things, mobile network, etc. (related to SG16, SG20), see Figure 9.

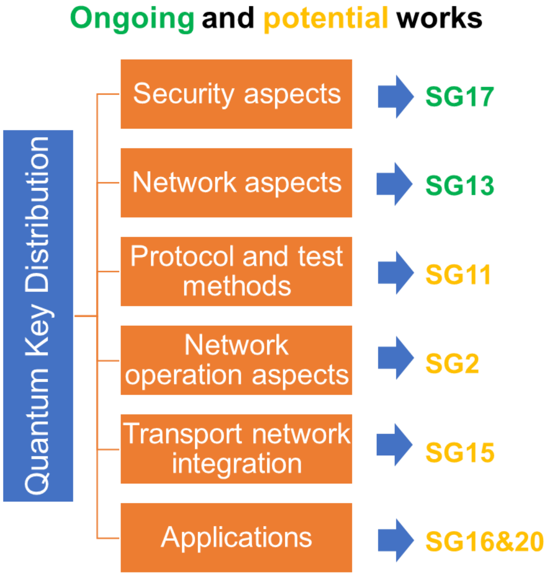

Ongoing and potential works
Quantum Key Distribution
Security aspects
SG17
Network aspects
SG13
Protocol and test methods
SG11
Network operation aspects
SG2
Transport network integration
SG15
Applications
SG16&20

Figure 9 – QKDN standardization aspects in the context of ITU-T

8.2 Key issues for QKDN standardization

QKDN is still a continuously evolving technology. The challenges for QKDN standardization exist from near term issues (e.g., how to ensure security and interoperability of trusted relay based QKD network) to medium- and long-term issues (e.g., how to reduce costs via integration of quantum and classical telecom networks, how to extend the applications of QKD, how to scale up the network via quantum relay), see Figure 10.

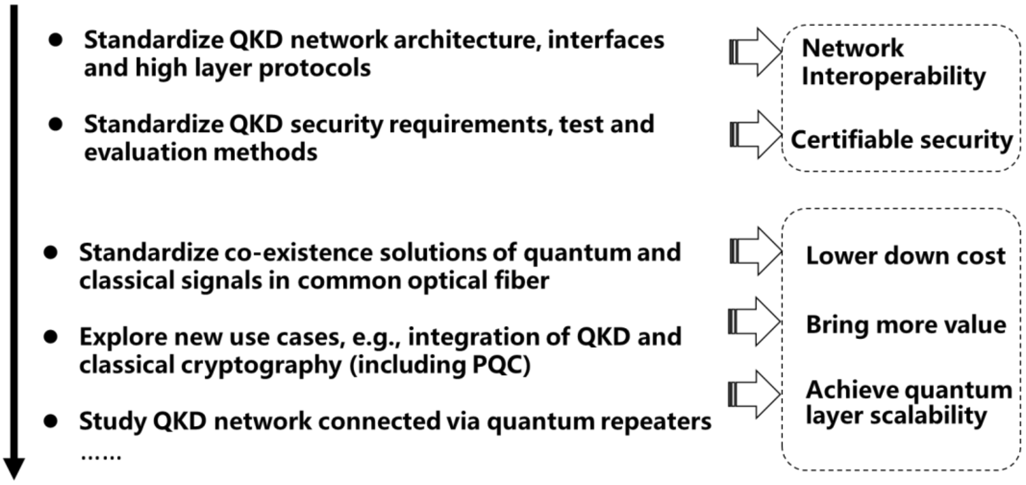

Standardize QKD network architecture, interfaces and high layer protocols
Standardize QKD security requirements, test and evaluation methods
Standardize co-existence solutions of quantum and classical signals in common optical fiber
Explore new use cases, e.g., integration of QKD and classical cryptography (including PQC)
Study QKD network connected via quantum repeaters
……
Network Interoperability
Certifiable security
Lower down cost
Bring more value
Achieve quantum layer scalability

Figure 10 – Near term to long term QKDN standardization perspective

Future work on QKDN standardization may cover aspects that could potentially resolve the issues highlighted below.

1) Issue 1: How can QKDN interoperability be ensured?

Interoperability is important for wide-area QKDNs to ensure that network and user devices from different vendors work seamlessly. Interoperability between QKD devices should be one of the most important issues to be resolved. As illustrated in Figure 10, there are two possible solutions to achieve multi-vendor QKD device interoperability:

- **Key management level interoperability:** Only needs to standardize the protocols for interfaces between KMs and QKD modules to enable the two hops of adjacent QKD links to use different vendor devices.
- **QKD link level interoperability:** Needs to standardize the protocols of all the interfaces between two QKD nodes, including quantum channels, key distillation channels, and key relay channels, to enable connectivity between QKD devices from different vendors.

Although the key management level interoperability can only achieve limited interoperability, it is easy to achieve and requires less standardization work. The QKD link level interoperability, on the other hand, can achieve full interoperability but requires standardization of the QKD protocol.

There is ongoing work in this direction, e.g., QKDN architecture and reference points have been specified in SG13, QKDN protocols are being studied in [b-QIT4N D2.3] and SG11 has initiated standardization on the QKDN protocol framework.

2) Issue 2: How can the cost of QKDN deployment be lowered?

Current QKD implementations require expensive fibre, racks, room resources and separate hardware devices. Reducing the cost of QKD deployment by as much as possible is a key element to its commercial development. Possible means for cost reduction include the co-existence of quantum and classical signals in a common optical fibre, integration of QKD modules into telecom network devices, etc. These technologies require deliberate design of the QKD transport system and integration with classical communication systems.

There is also ongoing work in this direction, e.g., initial discussions on QKD in SG15 and the QKDN transport technology study in [b-QIT4N D2.4].

3) Issue 3: How can QKD applications be extended to more valuable scenarios?

The current QKD applications are largely limited by their bulky hardware, strict quantum channel requirements, and limited functions of the QKD protocol, etc. To flourish the QKD industry, new QKD application scenarios and use cases need to be further identified and studied to explore more valuable business scenarios, e.g., satellite-based wide-area QKD, miniaturized and free space QKD, integration of QKD and classical cryptography solutions, e.g., PQC, blockchain.

[b-QIT4N D2.2] has reviewed and investigated new use cases of QKDN to facilitate possible future standardization in this direction.

4) Issue 4: How can the security of trusted-relay-based QKDN be ensured?

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

Currently, QKD security study is being pursued in ETSI, ITU-T and ISO/IEC JTC1. Work on security enhancement will always be an important topic for QKDN and new solutions including enhancement of trusted relaying techniques and development of MDI or quantum relay based QKDN should be explored in future.

5) Issue 5: How can QKDNs be scaled via quantum relay?

Although QKDNs can be constructed via trusted relay, this introduces potential security threats since quantum keys stored in the KM memories as classical bits are no longer guaranteed by quantum physics. The merger of quantum relay and quantum repeater technologies to realize scalable QKDNs is the ultimate secure quantum communication solution. The solutions and technical requirements for quantum relay and quantum repeater technologies need to be studied to prepare for the coming of new technologies to extend the reach of QKDNs in a real quantum manner.

Quantum relay technology is still far from being commercialized. The standardization study for a full quantum network has been initiated in IETF QIRG and FG-QIT4N WG1.

Appendix I

PQC study and standardization

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of PQC is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks.

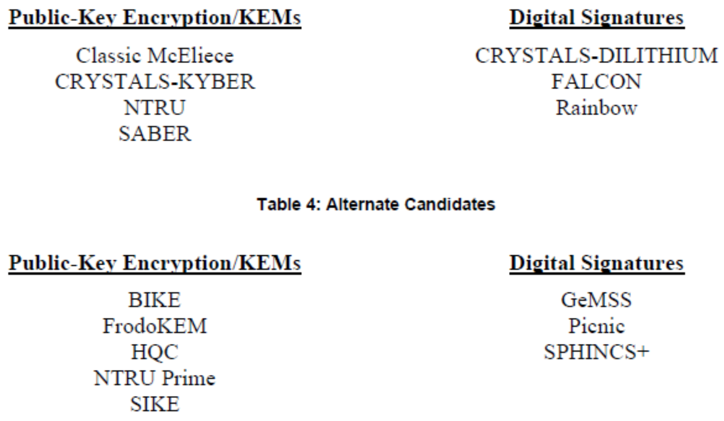
A large international community has emerged to address the issue of information security in a quantum computing future, in the hope that the public key infrastructure may remain intact by utilizing new quantum-resistant primitives. In the academic world, this new science bears the name "*Post-Quantum Cryptography2*" and is an active area of research with its own conference series, PQCrypto, which started in 2006. It has received substantial support from national funding agencies, most notably in the United States, Europe, and Japan, including through the EU PQCrypto and SAFEcrypto projects and the CREST Crypto-Math project in Japan.

These efforts have led to advances in fundamental research, paving the way for the deployment of post-quantum cryptosystems in the real world. In the past few years, industry and standards organizations have started their own activities in this field. Since 2013, ETSI has held several "Quantum-Safe Cryptography" workshops, in 2015, NIST held a workshop on "Cybersecurity in a Post-Quantum World" [b-NISTIR 8105] and in 2021, ITU-T FG-QIT4N co-organized a workshop with ETSI titled "Cybersecurity in the quantum era" which examined both QKD and PQC by discussing the merits and perceptions of each in the context of what may constitute a "good enough" cryptographic solution and the roles QKD and PQC play in a co-existing landscape [b-Webinar].

NIST is in the process of selecting one or more public-key cryptographic algorithms through a public competition-like process. The new public-key cryptography standards will specify one or more additional digital signature, public-key encryption, and key-establishment algorithms to augment FIPS 186-4, digital signature standard (DSS), as well as special publications SP 800-56A Revision 2, "*Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*" and SP 800-56B "*Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization*". It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers.

In November 2017, 82 candidate algorithms were submitted to NIST for consideration. Among these, 69 met both the minimum acceptance criteria and submission requirements and were accepted as first-round candidates on December 20, 2017, marking the beginning of the "First Round of the NIST Post-Quantum Cryptography Standardization Process". 26 candidate algorithms were announced on January 30, 2019, to progress to the second round of the competition, including 17 second-round candidate public-key encryption and key-establishment algorithms and 9 second-round candidates for digital signatures [b-NISTIR 8240].

In July 2020, the internal and external cryptanalysis, performance benchmarks, studies, and experiments involving the second-round candidates led NIST to the selection of 7 third-round finalists and 8 alternate candidates, as shown in Figure 11. The announcement of these schemes marks the beginning of the third round of the NIST PQC standardization process.



Public-Key Encryption/KEMs	Digital Signatures
Classic McEliece	CRYSTALS-DILITHIUM
CRYSTALS-KYBER	FALCON
NTRU	Rainbow
SABER	

Table 4: Alternate Candidates

Public-Key Encryption/KEMs	Digital Signatures
BIKE	GeMSS
FrodoKEM	Picnic
HQC	SPHINCS+
NTRU Prime	
SIKE	

Figure I.1 – Third round finalists and alternate candidates of NIST PQC competition [b-NISTIR 8309]

The third round is expected to last between 12 and 18 months and NIST held the third NIST PQC standardization conference in June 2021. NIST expects to select a small number of candidates for standardization by early 2022. To achieve this goal, the third round will serve as a final round for the first phase of standardization, though some schemes will remain under consideration for future standards [b-NISTIR 8309].

Bibliography

[b-Abellan] Abellan, C., Amaya, W., Domenech, D., Muñoz, P., Capmany, J., Longhi, S., Mitchell, M. and Pruneri, V. (2016), *Quantum entropy source on an InP photonic integrated circuit for random number generation*. Optica Vol. 3, No. 9, September, pp. 989–994.

[b-Agnesi] Agnesi, C. Lio, B., Cozzolino, D., Cardi, L., Bakir, B., Hassan, K., Frera, A., Ruggeri, A., Giudice, A., Vallone, G., Villoresi, P., Tosi, A., Rottwitt, K., Ding, Y. and Bacco D. (2019), *Hong-Ou-Mandel interference between independent III–V on silicon waveguide integrated lasers*. Optics Letters Vol. 44, No. 2, January, pp. 271-274.

[b-Aguado] Aguado, A., Lopez, V., Lopez, D., Momtchil, P., Poppe, A., Pastor, A., Folgueira, J. and Martín, V. (2019), *The Engineering of a SDN Quantum Key Distribution Network*. IEEE Comms. Mag, Julio, Special number "The Future of Internet", http://arxiv.org/abs/1907.00174

[b-ANSSI] ANSSI (2020), *Should Quantum Key Distribution be Used for Secure Communications?* ANSSI Technical Position Paper, May. https://www.ssi.gouv.fr/uploads/2020/05/anssi-technical_position_papers-qkd.pdf

[b-Battelle] Wallstreet online (2013), *Battelle Installs First Commercial Quantum Key Distribution Protected Network in U.S.* https://www.wallstreet-online.de/nachricht/6366901-battelle-installs-first-commercial-quantum-key-distribution-protected-network-u-s

[b-Bennett-1] Bennett, C., Bessette, F., Brassard, G., Salvail, L. and Smolin, J. (1992), *Experimental quantum cryptography*. Journal of Cryptology Vol. 5, January, pp. 3–28.

[b-Bennett-2] Bennett, C., Brassard, G. and Mermin, D. (1992), *Quantum cryptography without Bell's theorem*. Physical Review Letters Vol. 68, No. 5, February, pp. 557-559.

[b-BMBF] Bundesministerium für Bildung und Forschung (2018), *Quantentechnologien – von den Grundlagen zum Markt*. https://www.bmbf.de/upload_filestore/pub/Quantentechnologien.pdf

[b-Boaron] Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., Perrenoud, M., Gras, G., Bussières, F., Li, M., Nolan, D., Martin, A. and Zbinden, H. (2018), *Secure Quantum Key Distribution over 421 km of Optical Fibre*. Physical Review Letters Vol. 121, No. 121, November, pp. 190502.

[b-Briegel] Briegel, H.-J., Dür, W., Cirac, J. I. and Zoller, P. (1998), *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*. Physical Review Letters Vol. 81, No. 26, December, pp. 5932-5935.

[b-Bunandar] Bunandar, D., Lentine, A., Lee, C., Cai, H., Long, C., Boynton, N., Martinez, N., DeRose, C., Chen, C., Grein, M., Trotter, D., Starbuck, A., Pomerene, A., Hamilton, S., Wong, F., Camacho, R., Davids, P., Urayama, J. and Englund D. (2018), *Metropolitan quantum key distribution with silicon photonics*. Physical Review. Vol. 8, No. 021009, April.

[b-Calsamiglia] Calsamiglia, J. and Lütkenhaus, N. (2001), *Maximum efficiency of a linear-optical Bell-state analyzer*. Applied Physics B Vol. 72, January, pp. 67-71.

[b-Chatterjee] Chatterjee, R., Joarder, K., Chatterjee, S., Sanders, B. C. and Sinha, U. (2020), *qkdSim, a Simulation Toolkit for Quantum Key Distribution Including Imperfections: Performance Analysis and Demonstration of the B92 Protocol Using Heralded Photons*. Physical Review Applied, Vol. 14, No. 2.

[b-Chen-1] Chen, J.-P., Zhang, C., Yang, L., Jiang, C., Zhang, W., Hu, X., Jian-Yu, G., Yu, Z., Xu, H., Lin, J., Li, M., Chen, H., Li, H., You, L., Wang, Z., Wang, X., Zhang, Q. and Pan, J (2020), *Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km*. Physical Review Letters Vol. 124, No. 7, February.

[b-Chen-2] Chen, T., Liang, H., Liu, Y., Cai, W., Ju, L., Liu, W., Wang, J., Yin, H., Chen, K., Chen, Z., Peng, C. and Pan, J. (2009), *Field test of a practical secure communication network with decoy-state quantum cryptography*. Optics Express, Vol. 17, No. 8, pp. 6540-6549.

[b-Chen-3] Chen, T, Wang, J., Liang, H., Liu, W., Liu, Y., Jiang, X., Wang, Y., Wan, X., Cai, W., Ju, L., Chen, L., Wang, L., Gao, Y., Chen, K., Peng, C., Chen, Z. and Pan, J. (2010), *Metropolitan all-pass and inter-city quantum communication network*. Optics Express Vol. 18, No. 26, August, pp. 27217-27225.

[b-Chen-4] Chen Y. (2019), *Quantum information technology development in China*. In ITU Workshop on Quantum Information Technology for Networks, Shanghai, China.https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Yuao_Chen_Presentation.pdf

[b-Comandar] Comandar, L, Lucamarini, M., Fröhlich, B., Dynes, J., Sharpe, A., Tam, S., Yuan, Z., Penty, R., and Shields, A. (2016), *Quantum cryptography without detector vulnerabilities using optically-seeded lasers*. Nature Photonics Vol.10, No. 5, April, pp. 312-315.

[b-Csa] Government of Canada, *Quantum Encryption and Science Satellite (QEYSSat)*. Retrieved on 24 November 2021. https://www.asc-csa.gc.ca/eng/satellites/qeyssat.asp

[b-CSIRO] CSIRO Futures (2020), *Growing Australia's Quantum Technology Industry*. Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia. https://www.csiro.au/en/Showcase/quantum

[b-Dai] Dai, H., Shen, Q., Wang, C., Li, S., Liu, W., Cai, W., Liao, S., Ren, J., Yin, J., Chen, Y., Zhang, Q., Xu, F., Peng, C. and Pan, J. (2020), *Towards satellite-based quantum-secure time transfer*. Nature Physics Vol. 16, May, pp. 848–852.

[b-Deutsch] Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S., and Sanpera, A. (1996), *Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels*. Physical Review Letters Vol. 77, No. 13, September, pp. 2818-2821.

[b-Ding] Ding, Y., Bacco, D., Dalgaard, K., Cai, X., Zhou, X., Rottwitt, K. and Oxenløwe, L (2017), *High-dimensional quantum key distribution based on multicore fibre using silicon photonic integrated circuits*. npj Quantum Information. Vol. 3, No. 25, June.

[b-Dixon] Dixon, A., Yuan, Z., Dynes, J., Sharpe, A. and Shields, A. (2008), *Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate*. Optics Express Vol. 16, No. 23, November, pp. 18790-18797.

[b-DoD] Department of Defense, Defense Science Board (2019), *Applications of Quantum Technologies*.

[b-Duan] Duan, L., Lukin, M., Cirac, J. and Zoller, P. (2001), *Long-distance quantum communication with atomic ensembles and linear optics*. Nature Vol. 414, November pp. 413-418.

[b-ETSI GS QKD] ETSI GS QKD 011 V1.1.1 (2016), *Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems*.

[b-EU-1] Huebel, H. (2019), *European Quantum Technology FET Flagship*. In ITU Workshop on Quantum Information Technology for Networks, Shanghai, China. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Hannes_Huebel_Presentation.pdf

[b-EU-2] European Commission (2020), *Strategic research agenda*. European Quantum Flagship, March. https://ec.europa.eu/digital-single-market/en/news/new-strategic-research-agenda-quantum-technologies

[b-EU-3] European Commission (2019), *Technical agreement signed for a European plan on quantum communication infrastructure*. European Union. https://digital-strategy.ec.europa.eu/en/news/technical-agreement-signed-european-plan-quantum-communication-infrastructure

[b-EU-4] European Commission (2019), *Open European Quantum Key Distribution*. European Union. https://openqkd.eu/

[b-Fang] Fang, X., Zeng, P., Liu, H., Zou, M., Wu, W., Tang, Y., Sheng, Y., Xiang, Y., Zhang, W., Li, H., Wang, Z., You, L., Li, M., Chen, H., Chen, Y., Zhang, Q., Peng, C., Ma, X., Chen, T. and Pan, J. (2020), *Implementation of quantum key distribution surpassing the linear rate-transmittance bound*. Nature Photonics Vol. 14, March, pp. 422-425.

[b-Fedorov] Fedorov, A., Akimov, A., Biamonte, J., Kavokin, A., Khalili, F., Kiktenko, E., Kolachevsky, N., Kurochkin, Y., Lvovsky, A., Rubtsov, A., Shlyapnikov, G., Straupe, S., Ustinov, A. and Zheltikov, A. (2019), *Quantum technologies in Russia*. Quantum Science and Technology Vol. 4, pp. 040501.

[b-Ferreira] Ferreira da Silva, T., Vitoreti, D., Xavier, G., do Amaral, G., Temporão, G. and von der Weid, J. (2013), *Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits*. Physical Review A Vol. 88, No. 5, November.

[b-Fröhlich-1] Fröhlich, B., Dynes, J., Lucamarini, M., Sharpe, A., Yuan, Z. and Shields A. (2013), *A quantum access network*. Nature Vol. 501, September, pp. 69-72.

[b-Fröhlich-2] Fröhlich, B., Lucamarini, M., Dynes, J., Comandar, L., Tam, W., Plews, A., Sharpe, A., Yuan, Z. and Shields, A. (2017), *Long-distance quantum key distribution secure against coherent attacks*. Optica 4, No. 1, January, pp. 163-167.

[b-Fujiwara] Fujiwara, M., Waseda, A., Nojima, R., Moriai, S., Ogata, W. and Sasaki, M. (2016), *Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing*. Scientific Reports Vol. 6, No. 28988.

[b-Gisin] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H. (2002), *Quantum cryptography*, Reviews of Modern Physics Vol. 74, January pp. 145–195 [b-GISTDA] Geo-Informatics and Space Technology Development Agency (GISTDA). *Earth Space System: ESS*. Retrieved on 24 November 2021, http://learn.gistda.or.th/ess2/

[b-Grosshans] Grosshans, F. and Grangier, P. (2002), *Continuous Variable Quantum Cryptography Using Coherent States.* Physical Review Letters Vol. 88, No. 5, January.

[b-Guan] Guan, J.-Y., Cao, Z., Liu, Y., Shen-Tu, G.-L., Pelc, J. S., Fejer, M. M., Peng, C.-Z., Ma, X., Zhang, Q. and Pan, J.-W. (2015), *Experimental passive round-robin differential phase-shift quantum key distribution*. Physical Review Letters, Vol. 114, No. 18, p. 180502.

[b-Günthner] Günthner, K., Khan, I., Elser, D., Stiller, B., Bayraktar, Ö., Müller, C., Saucke, K., Tröndle, D., Heine, F., Seel, S., Greulich, P., Zech, H., Gütlich, B., Philipp-May, S., Marquardt, C. and Leuchs, G. (2017), *Quantum-limited measurements of optical signals from a geostationary satellite.* Optica Vol. 4, No. 6, June, pp. 611-616.

[b-Guo] Guo, Y. (2019), *Application in power industry promotes the development of quantum cryptography technology*. In ITU Workshop on Quantum Information Technology for Networks, Shanghai, China. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Yonghe_Guo_Presentation.pdf

[b-Hasegawa] Hasegawa, Y., Ikuta, R., Matsuda, N., Tamaki, K., Lo, H., Yamamoto, T., Azuma, K. and Imoto, N. (2019). *Experimental time-reversed adaptive Bell measurement towards all-photonic quantum repeaters*. Nature Communications Vol. 10, No. 378, January.

[b-Honjo] Honjo, T., Inoue, K. and Takahashi, T. (2004), *Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach–Zehnder interferometer*, Optics Letters. Vol. 29, December, pp. 2797–2799.

[b-Huang-1] Huang, D., Huang, P., Lin, D., Wang, C. and Zeng, G. (2015), *High-speed continuous-variable quantum key distribution without sending a local oscillator*. Optics letters Vol. 40, No. 16, pp. 3695-3698.

[b-Huang-2] Huang, D., Lin, D., Wang, C., Liu, W., Fang, S., Peng, J., Huang, P. and Zeng, G. (2015), *Continuous-variable quantum key distribution with 1 Mbps secure key rate*. Optics Express Vol. 23, No. 13, June, pp. 17511-17519.

[b-Hughes] Hughes, R., Nordholt, J., McCabe, K., Newell, R., Peterson, C. and Somma, R. (2013), *Network-Centric Quantum Communications*. Frontiers in Optics, OSA Technical Digest (online) (Optical Society of America, 2013), paper FW2C.1.

[b-India] Office of the Principal Scientific Adviser to the Government of India, Quantum Technologies. https://www.psa.gov.in/technology-frontiers/quantum-technologies/346.

[b-Islam] Islam, N., Lim, C., Cahall, C., Kim, J. and Gauthier, D. (2017), *Provably secure and high-rate quantum key distribution with time-bin qudits*. Science Advances Vol. 3, November, e1701491.

[b-Jiang] Jiang, L., Taylor, J. M., Nemoto, K., Munro, W. J., Van Meter, R and Lukin, M. D (2009), *Quantum repeater with encoding*," Physical Review A Vol. 79, No. 3, March.

[b-Jin] Jin, X., Ren, J., Yang, B. Yi, Z., Zhou, F., Xu, X., Wang, S., Yang, D., Hu, Y., Jiang, S., Yang, T., Yin, H., Chen, K., Peng, C. and Pan, J. (2010), *Experimental free-space quantum teleportation*. Nature Photonics Vol. 4, May, pp. 376–381.

[b-Jouguet] Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. and Diamanti, E. (2013), *Experimental demonstration of long-distance continuous-variable quantum key distribution*. Nature photonics Vol. 7, No. 5, April, pp. 378-381.

[b-Kaneda] Kaneda, F., Xu, F., Chapman, J. and Kwiat, P. (2017), *Quantum-memory-assisted multi-photon generation for efficient quantum information processing*. Optica Vol. 4, No. 9, August, pp. 1034-1037.

[b-Khan] Khan, I., Heim, B., Neuzner, A. and Marquardt, C. (2018), *Satellite-Based QKD*. Optics and Photonics News, Vol. 29, No. 2, February, pp. 26-33.

[b-Korzh] Korzh, B., Lim, C., Houlmann, R., Gisin, N., Li, M., Nolan, D., Sanguinetti, B., Thew, R. and Zbinden, H. (2015), *Provably secure and practical quantum key distribution over 307 km of optical fibre*. Nature Photonics Vol. 9, February, pp. 163-168.

[b-Kreinberg] Kreinberg, S., Novik, P., Koltchanov, I. and Richter, A. (2020), *Modelling weak-coherent QKD systems using a classical simulation framework*. In Conference on Lasers and Electro-Optics, Optical Society of America (OSA) Technical Digest, May.

[b-Kumar] Kumar, R., Qin, H. and Alléaume, R. (2015), *Coexistence of continuous variable QKD with intense DWDM classical channels*. New Journal of Physics, Vol. 17, April, p. 043027.

[b-Lancho] Lancho, D., Martinez, J., Elkouss, D., Soto, M. and Martin, V. (2009), *QKD in Standard Optical Telecommunications Networks*. In International Conference on Quantum Communication and Quantum Networking (QuantumComm 2009), October 26-30, Naples, Italy, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 36, pp. 142-149.

[b-Lee] Lee, C., Zhang, Z., Steinbrecher, G., Zhou, H., Mower, J., Zhong, T., Wang, L., Hu, X., Horansky, R., Verma, V., Lita, A., Mirin, R., Marsili, F., Shaw, M., Nam, S., Wornell, G., Wong, F., Shapiro, J. and Englund, D. (2014), *Entanglement-based quantum communication secured by nonlocal dispersion cancellation*. Physical Review A Vol. 90, No. 6, p. 062331.

[b-Li-1] Li, Z., Zhang, R., Yin, X., Liu, L., Hu, Y., Fang, Y., Fei, Y., Jiang, X., Zhang, J., Li, L., Liu, N., Xu, F., Chen, Y. and Pan, J. (2019). *Experimental quantum repeater without quantum memory*. Nature Photonics Vol. 13, June, pp. 644–648.

[b-Li-2] Li, Y., Cao, Y., Dai, H., Lin, J., Zhang, Z., Chen, W., Xu, Y., Guan, J., Liao, S., Yin, J., Zhang, Q., Ma, X., Peng, C. and Pan, J. (2016), *Experimental round-robin differential phase-shift quantum key distribution*. Physical Review A Vol. 93, No. 3, March, p. 030302.

[b-Liao-1] Liao, S., Cai, W., Liu, W., Zhang, L., Li, Y., Ren, J., Yin, J., Shen, Q., Cao, Y., Li, Z., Li, F., Chen, X., Sun, L., Jia, J., Wu, J., Jiang, X., Wang, J., Huang, Y., Wang, Q., Zhou, Y., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y., Liu, N., Wang, X., Zhu, Z., Lu, C., Shu, R., Peng, C., Wang J-Y. and Pan, J. (2017) *Satellite-to-ground quantum key distribution*. Nature 549, August, pp. 43–47.

[b-Liao-2] Liao, S., Lin, J., Ren, J., Liu, W., Qiang, J., Yin, J., Li, Y., Shen, Q., Zhang, L., Liang, X., Yong, H., Li, F., Yin, Y., Cao, Y., Cai, W., Zhang, W., Jia, J., Wu, J., Chen, X., Zhang, S., Jiang, X., Wang, J., Huang, Y., Wang, Q., Ma, L., Li, L., Pan, G., Zhang, Q., Chen. Y., Lu, C., Liu, N., Ma, X., Shu, R., Peng, C., Wang, J. and Pan, J. (2017), *Space-to-Ground Quantum Key Distribution Using a Small-Sized Payload on Tiangong-2 Space Lab*. Chinese Physics Letters, Vol. 34, No. 9. 090302.

[b-Liao-3] Liao, S., Cai, W., Handsteiner, J., Liu, B., Yin, J., Zhang, L., Dominik, R., Matthias, F., Ren, J., Liu, W, Li, Y., Shen, Q., Cao, Y., Li, F., Wang, J., Huang, Y., Deng, L., Xi, T., Ma, L., Hu, T., Li, L., Liu, N., Koidl, F., Wang, P., Chen, Y., Wang, X., Steindorfer, M., Kirchner, G., Lu, C., Shu, R., Ursin, R., Scheidl, T., Peng, C., Wang, J., Zeilinger, A. and Pan, J. (2018), *Satellite-relayed intercontinental quantum network*. Physical Review Letters Vol. 120, No. 3, January.

[b-Liao-4] Liao, S., Yong, H., Liu, C., Shentu, G., Li, D., Lin, J., Dai, H., Zhao, S., Li, B., Guan, J., Chen, W., Gong,Y., Li, Y., Lin, Z., Pan, G., Pelc, J., Fejer, M., Zhang, W., Liu, W., Yin, J., Ren, J., Wang, X., Zhang, Q., Peng, C. and Pan, J. (2017) *Long-distance free-space quantum key distribution in daylight towards inter-satellite communication*. Nature Photonics Vol. 11, July, pp. 509-513.

[b-Liu-1] Liu, Y., Chen, T., Wang, J., Cai, W., Wan, X., Chen, L., Wang, J., Liu, S., Liang, H., Yang, L., Peng, C., Chen, K., Chen, Z. and Pan, J. (2010), *Decoy-state quantum key distribution with polarized photons over 200 km*. Optics Express, Vol. 18, No. 8, April, pp. 8587-8594.

[b-Liu-2] Liu, Y., Chen, T., Wang, L., Liang, H., Shentu, G., Wang, J., Cui, K., Yin, H., Liu, N., Li, L., Ma, X., Pelc, J., Fejer, M., Peng, C., Zhang, Q. and Pan, J. (2013), *Experimental Measurement-Device-Independent Quantum Key Distribution*. Physical Review Letters Vol. 111, No. 13, September, p. 130502.

[b-Liu-3] Liu, H., Wang, J., Ma, H. and Sun, S. (2018), *Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration*. Optica Vol. 5, No. 8, July, pp. 902-909.

[b-Liu-4] Liu, H., Wang, W., Wei, K., Fang, X., Li, L., Liu, N., Liang, H., Zhang, S., Zhang, W., Li, H., You, L., Wang, Z., Lo, H., Chen, T., Xu, F., and Pan, J. (2019), *Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum Key Distribution over Asymmetric Channels*. Physical Review Letters Vol. 122, No. 16, April, p. 160501.

[b-Liu-5] Liu, Y., Yu, Z., Zhang, W., Guan, J., Chen, J., Zhang, C., Hu, X., Li, H., Jiang, C., Lin, J., Chen, T., You, L., Wang, Z., Wang, X., Zhang, Q. and Pan, J. (2019), *Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending*. Physical Review Letters, Vol. 123, No. 10, p.100505.

[b-Lucamarini-1] Lucamarini, M., Yuan, Z., Dynes, J. and Shields, A. (2018) *Overcoming the rate–distance limit of quantum key distribution without quantum repeaters*. Nature Vol. 557, May, pp. 400–403.

[b-Lucamarini-2] Lucamarini, M., Patel, K., Dynes, J., Fröhlich, B., Sharpe, A., Dixon, A., Yuan, Z., Penty, R. and Shields, A. (2013), *Efficient decoy-state quantum key distribution with quantified security*. Optics Express Vol. 21, No. 21, October, pp. 24550-24565.

[b-Ma] Ma, C., Sacher, W., Tang, Z., Mikkelsen, J., Yang, Y., Xu, F., Lo, H. and Poon, J (2016), *Integrated silicon photonic transmitter for polarization-encoded quantum key distribution*. Optica Vol. 3, No. 11, June, pp. 1274–1278.

[b-Mailloux] Mailloux, L. O., Morris, J. D., Grimaila, M. R., Hodson, D. D., Jacques, D. R., Colombi, J. M., Mclaughlin, C. V., Holes, J. A. (2015), *A Modeling Framework for Studying Quantum Key Distribution System Implementation Nonidealities*. IEEE Access Vol. 3, pp. 110-130.

[b-Martino] Martino, T. and Lewis, A., (2019). *Quantum Key Distribution in-field implementations*. European Commission JRC Technical Report 118150.

[b-McKinsey] McKinsey & Company (2021), *The Quantum Technology Monitor: Facts and Figures*.

[b-Minder] Minder, M., Pittaluga, M., Roberts, G., Lucamarini, M., Dynes, J. and Yuan, Z., Shields, A. (2019), *Experimental quantum key distribution beyond the repeaterless secret key capacity*. Nature Photonics, Vol. 13, May.

[b-Mirhosseini] Mirhosseini, M., Magaña-Loaiza, O., O'Sullivan, M., Rodenburg, B., Malik, M., Lavery, M., Padgett, M., Gauthier, D. and Boyd, R. (2015), *High-dimensional quantum cryptography with twisted light*. New Journal of Physics, Vol. 17, March, p. 033033.

[b-Mitacs] *Mitacs Projects - RBC-Toronto Quantum Key Distribution Network Development.* Retrieved on 24 November 2021.
https://www.mitacs.ca/en/projects/rbc-toronto-quantum-key-distribution-network-development

[b-Munro-1] Munro, W., Azuma, K., Tamaki, K. and Nemoto, K. (2015), *Inside Quantum Repeaters*. In IEEE Journal of Selected Topics in Quantum Electronics Vol. 21, No. 3, May-June, pp. 78-90.

[b-Munro-2] Munro, W., Stephens, A., Devitt, S., Harrison, K. and Nemoto, K. (2012), *Quantum communication without the necessity of quantum memories*. Nature Photonics Vol. 6, October, pp. 777-781.

[b-NAS] National Academies of Sciences, Engineering, and Medicine (2019), *Quantum Computing: Progress and Prospects.* The National Academies Press, Washington, DC.

[b-NASA] NASA (2020), *Workshop on Space Quantum Communications and Networks Agenda: Developing the Roadmap to Quantum Communications in Space*.
https://www.nasa.gov/sites/default/files/atoms/files/draft_agenda_workshop_on_space_quantum_communications_and_networks_01.21.2020.pdf

[b-NCSC] NCSC (2020), *Quantum security technologies*. White Paper, March.
https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

[b-NISTIR 8105] Chen, L., Jordan, S., Liu, Y., Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. (2016), *Report on Post-Quantum Cryptography.* NISTIR 8105, April.

[b-NISTIR 8240] Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D. and Liu, Y. (2019), *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. NISTIR 8240, January.

[b-NISTIR 8309] Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A. and Smith-Tone, D. (2020), *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. NISTIR 8309, July.

[b-NRC] National Research Council (2012), NASA Space Technology Roadmaps and Priorities: Restoring NASA's Technological Edge and Paving the Way for a New Era in Space. Washington, DC: The National Academies Press. https://doi.org/10.17226/13354.

[b-NSA] NSA CSS, *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*. Retrieved 15 February 2021. https://www.nsa.gov/what-we-do/cybersecurity/quantum-key-distribution-qkd-and-quantum-cryptography-qc/

[b-NXPO-1] Office of the National Council for Higher Education, Science, Research and Innovation Policy Council (NXPO) (2021). *Quantum research, November 15 version*. Retrieved on 24 November 2021. https://www.nxpo.or.th/B/quantum-research

[b-NXPO-2] Office of the National Council for Higher Education, Science, Research and Innovation Policy Council (NXPO). *Frontier research.* Retrieved on 24 November 2021. https://www.nxpo.or.th/th/en/frontier-research-2

[b-Oi] Oi, D. K., Ling, A., Vallone, G., Villoresi, P., Greenland, S., Kerr, E., Macdonald, M., Weinfurter, H., Kuiper, H., Charbon, E. and Ursin, R. (2017). *CubeSat quantum communications mission*. EPJ Quantum Technology Vol. 4, No. 6, April.

[b-OIDA] OIDA (2020), OIDA Quantum Photonics Roadmap: Every Photon Counts. OIDA Report, 3.

[b-Peev] Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J., Fasel, S., Fossier, S., Fürst, M., Gautier, J., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y., Hentschel, M., Hübel, H., Humer, G., Länger, T., Legré, M., Lieger, R., Lodewyck, J., Lorünser, T., Lütkenhaus, N., Marhold, A., Matyus, T., Maurhart, O., Monat, L., Nauerth, S., Page, J., Poppe, A., Querasser, E., Ribordy, G., Robyr, S., Salvail, L., Sharpe, A., Shields, A., Stucki, D., Suda, M., Tamas, C., Themel, T., Thew, R., Thoma, Y., Treiber, A., Trinkler, P., Tualle-Brouri, R., F., Walenta, N., Weier, H., Weinfurter, H., Wimberger, I., Yuan, Z., Zbinden, H. and Zeilinger A. (2009), *The SECOQC quantum key distribution network in Vienna*. New Journal of Physics, Vol. 11, July.

[b-Peng] Peng, C., Zhang, J., Yang, D., Gao, W., Ma, H., Yin, H., Zeng, H., Yang, T., Wang, X. and Pan, J (2007), *Experimental long-distance decoy-state quantum key distribution based on polarization encoding*. Physical Review Letters Vol. 98, No. 1, January.

[b-Pirandola-1] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P. and Wallden, P. (2020), *Advances in Quantum Cryptography*. Advances in Optics and Photonics Vol. 12, No. 4, December, pp. 1012-1236.

[b-Pirandola-2] Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, C., Braunstein, S., Lloyd, S., Gehring, T., Jacobsen, C. and Andersen, U. (2015), *High-rate measurement-device-independent quantum cryptography*. Nature Photonics Vol. 9, May, pp. 397-402.

[b-QEP] Quantum Engineering Programme. https://qepsg.org/

[b-QDNL] Quantum Delta Nederland (2019), *National Agenda for Quantum Technology*. https://qutech.nl/wp-content/uploads/2019/09/NAQT-2019-EN.pdf

[b-Qi-1] Qi, B., Lougovski, P., Pooser, R., Grice, W. and Bobrek, M. (2015), *Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection*. Physical Review X Vol. 5, No. 4, p. 041009.

[b-Qi-2] Qi, B, Lo, H.-K., Lim, C., Siopsis, G., Chitambar, E., Pooser, R., Evans, P. and Grice, W. (2015). *Free-space reconfigurable quantum key distribution network*. In 2015 IEEE International Conference on Space Optical Systems and Applications (ICSOS), pp.1-6.

[b-QIT4N D2.2] ITU-T Technical Report (2021), Quantum information technology for network use cases: Quantum key distribution network.

[b-QIT4N D2.3] ITU-T Technical Report (2021), *Quantum key distribution network protocols*.

[b-QIT4N D2.4] ITU-T Technical Report (2021), Quantum key distribution network transport technologies.

[b-QuantumSG] QuantumSG (2019), *Quantum Technologies in Singapore – preparing for the future*. https://quantumsg.org/preparing-future/

[b-QuST] Goverment of India Ministry of Science & Technology (2017), Interdisciplinary Cyber Physical Systems (ICPS) Division Detailed Call for Proposals (CFP) on Quantum Information Science and Technology (QuST) Programme. https://dst.gov.in/callforproposals/interdisciplinary-cyber-physical-systems-icps-division-detailed-call-proposals-cfp

[b-QXchange-1] Quantum Xchange, *Quantum Network from Boston to Washington DC in the Works*. Retrieved on 24 November 2021. https://quantumxc.com/media-coverage/quantum-network-from-boston-to-washington-dc-in-the-works/

[b-QXchange-2] Quantum Xchange (2019), *Quantum Xchange Breaks Final Barriers to Make Quantum Key Distribution (QKD) Commercially Viable with the Launch of Phio TX*. https://quantumxc.com/press-release/quantum-xchange-breaks-final-barriers-to-make-quantum-key-distribution-qkd-commercially-viable-with-the-launch-of-phio-tx/

[b-Ralph] Ralph, T. (1999), *Continuous variable quantum cryptography*. Physical Review A, Vol. 61, No. 1, December.

[b-Roger] Roger, T., Paraiso, T., Marco, I., Marangon, D., Yuan, Z. and Shields, A. (2019), *Real-time interferometric quantum random number generation on chip*. Journal of the Optical Society of America B Vol. 36, No. 3, June, pp. B137–B142.

[b-Rosenberg-1] Rosenberg, D., Harrington, J., Rice, P., Hiskett, P., Peterson, C., Hughes, R., Lita, A., Nam, S. and Nordholt, J. (2007), *Long-distance decoy-state quantum key distribution in optical fibre*. Physical Review Letters Vol. 98, No. 1.

[b-Rosenberg-2] Rosenberg, D., Peterson, C., Harrington, J., Rice, P., Dallmann, N., Tyagi, K., McCabe, K., Nam, S., Baek, B., Hadfield, R., Hughes, R. and Nordholt, J. (2009), *Practical long-distance quantum key distribution system using decoy levels*. New Journal of Physics, Vol. 11, April, 045009.

[b-Rubenok] Rubenok, A., Slater, J., Chan, P., Lucio-Martinez, I. and Tittel, W. (2013), *Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks*. Physical Review Letters Vol. 111, No. 13, September, p. 130501.

[b-Saglamyurek] Saglamyurek, E., Sinclair, N., Jin, J., Slater, J., Oblak, D., Bussières, F., George, M., Ricken, R., Sohler, W. and Tittel, W. (2011), *Broadband waveguide quantum memory for entangled photons*. Nature Vol. 469, January, pp. 512-515.

[b-Sasaki] Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K., Takeoka, M., Miki, S., Yamashita, T., Wang, Z., Tanaka, A., Yoshino, K., Nambu, Y., Takahashi, S., Tajima, A., Tomita, A., Domeki, T., Hasegawa, T., Sakai, Y., Kobayashi, H., Asai, T., Shimizu, K., Tokura, T., Tsurumaru, T., Matsui, M., Honjo, T., Tamaki, K., Takesue, H., Tokura, Y., Dynes, J., Dixon, A., Sharpe, A., Yuan, Z., Shields, A., Uchikoga, S., Legré, M., Robyr, S., Trinkler, P., Monat, L., Page, J., Ribordy, G., Poppe, A., Allacher, A., Maurhart, O., Länger, T., Peev, M., and Zeilinger, A. (2011), *Field test of quantum key distribution in the Tokyo QKD Network*. Optics Express Vol. 19, No. 11, May, pp. 10387-10409.

[b-Schmitt] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R, Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J., Zeilinger, A. and Weinfurter, H. (2007), *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km*. Physical Review Letters Vol. 98, No. 1, January, pp. 010504

[b-Semenenko] Semenenko, H., Sibson, P., Thompson, M. and Erven C. (2019), *Interference between independent photonic integrated devices for quantum key distribution*. Optics Letters. Vol. 44, No. 2, January, pp. 275–278

[b-Sharman] Sharman, K., Asadi, F. K., Wein, S. C. and Simon, C. (2021), Quantum repeaters based on individual electron spins and nuclear-spin-ensemble memories in quantum dots. Quantum Vol. 5, p. 570

[b-Shi] Shi, H. (2019), *QKD standardization in ISO/IEC JTC1/SC27 - An introduction of ISO/IEC 23837*. In ITU Workshop on Quantum Information Technology (QIT) for Networks, Shanghai, China.

[b-Sibson-1] Sibson, P., Erven, C., Godfrey, M., Miki, S., Yamashita, T., Fujiwara, M., Sasaki, M., Terai, H., Tanner, M. G., Natarajan, C. M., Hadfield, R. H., O'Brien, J. L., and Thompson, M. G., (2017), *Chip-based quantum key distribution*. Nature Communications. Vol. 8, No. 13984, February.

[b-Sibson-2] Sibson, P., Kennard, J., Stanisic, S., Erven, C., O'Brien, J. and Thompson, M. (2017), *Integrated silicon photonics for high-speed quantum key distribution*. Optica Vol. 4, No. 2, January, pp. 172–177.

[b-Sit] Sit, A., Bouchard, F., Fickler, R., Gagnon-Bischoff, J., Larocque, H., Heshami, K., Elser, D., Peuntinger, C., Günthner, K., Heim, B., Marquardt, C., Leuchs, G., Boyd, R. and Karimi, E. (2017), *High-dimensional intracity quantum cryptography with structured photons*. Optica Vol. 4, No. 9, August, pp. 1006-1010.

[b-Soh] Soh, D., Brif, C., Coles, P., Lütkenhaus, N., Camacho, R., Urayama, J. and Sarovar, M. (2015), *Self-Referenced Continuous-Variable Quantum Key Distribution Protocol*. Physical Review X Vol. 5, No. 4, October, p. 041010.

[b-Takenaka] Takenaka, H., Carrasco-Casado, A., Fujiwara, M., Kitamura, M., Sasaki, M. and Toyoshima, M. (2017) *Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite*. Nature Photonics Vol. 11, July, pp. 502–508.

[b-Takesue] Takesue, H., Sasaki, T., Tamaki, K. and Koashi, M. (2015), *Experimental quantum key distribution without monitoring signal disturbance*. Nature Photonics Vol. 9, September, pp. 827-831.

[b-Tang-1] Tang, Z., Chandrasekara, R., Tan, Y. C., Cheng, C., Sha, L., Hiang, G. C., Oi, D. K. and Ling, A. (2016) *Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite*. Physical Review Applied Vol. 5, p. 054022.

[b-Tang-2] Tang, Z., Liao, Z., Xu, F., Qi, B., Qian, L. and Lo, H. (2014), *Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution*. Physical Review Letters Vol. 112, No. 19, p. 190503.

[b-Tang-3] Tang, Y., Yin, H., Chen, S., Liu, Y., Zhang, W., Jiang, X., Zhang, L., Wang, J., You, L., Guan, J., Yang, D., Wang, Z., Liang, H., Zhang, Z., Zhou, N., Ma, X., Chen, T., Zhang, Q. and Pan, J. (2014), *Measurement-Device-Independent Quantum Key Distribution over 200 km*. Physical Review Letters Vol. 113, No. 19, November, p. 190501.

[b-Tang-4] Tang, Y., Yin, H., Chen, S., Liu, Y., Zhang, W., Jiang, X., Zhang, L., Wang, J., You, L., Guan, J., Yang, D., Wang, Z., Liang, H., Zhang, Z., Zhou, N., Ma, X., Chen, T., Zhang, Q. and Pan, J. (2015), *Field Test of Measurement-Device-Independent Quantum Key Distribution*. IEEE Journal of Selected Topics in Quantum Electronics Vol. 21, No. 3, May-June, pp. 116-122.

[b-Tang-5] Tang, Y., Yin, H., Zhao, Q., Liu, H., Sun, X., Huang, M., Zhang, W., Chen, S., Zhang, L., You, L., Wang, Z., Liu, Y., Lu, C., Jiang, X., Ma, X., Zhang, Q., Chen, T. and Pan, J. (2016), *Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network*. Physical Review X Vol. 6, No. 1, March, p. 011024

[b-Tang-6] Tang, G., Sun, S., Xu, F., Chen, H., Li, C. and Liang, L. (2016), *Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution*. Physical Review A Vol. 94, No. 3, September, p. 032326.

[b-Teh] Teh, N. J. (2018), *Innovate UK Global Expert Mission, Quantum Technologies in Canada 2018*. https://prod5.assets-cdn.io/event/4884/assets/8415902632-532109e749.pdf [b-Thompson] Thompson, M. G. (2019), *Large-scale integrated quantum photonic technologies for communications and computation*. In Optical Fibre Communication Conference (OFC) 2019, OSA Technical Digest, 2019), paper W3D.3.

[b-UK] UK National Quantum Technologies Programme (2015), *A roadmap for quantum technologies in the UK*, Innovate UK and the Engineering and Physical Sciences Research Council, September. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/470243/InnovateUK_QuantumTech_CO004_final.pdf

[b-Ursin] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Ömer, B., Fürst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., and Zeilinger, A. (2007), *Entanglement-based quantum communication over 144 km*, Nature Physics Vol. 3, June, pp.481-486.

[b-Valivarthi-1] Valivarthi, R., Lucio-Martinez, I., Chan, P., Rubenok, A., John, C., Korchinski, D., Duffin, C., Marsili, F., Verma, V., Shaw, M., Stern, J., Nam, S., Oblak, D., Zhou, Q., Slater, J. and Tittel, W. (2015), *Measurement-device-independent quantum key distribution: from idea towards application*. Journal of Modern Optics Vol. 62, No. 14, March, pp. 1141-1150.

[b-Valivarthi-2] Valivarthi, R., Zhou, Q., John, C., Marsili, F., Verma, V., Shaw, M., Nam, S., Oblak, D. and Tittel, W. (2017), *A cost-effective measurement-device-independent quantum key distribution system for quantum networks*. Quantum Science and Technology Vol. 2, No. 4.

[b-Vergoossen] Tom Vergoossen, Sergio Loarte, Robert Bedington, Hans Kuiper, Alexander Ling, *Modelling of satellite constellations for trusted node QKD networks*. Acta AstronauticaVolume 173, Pages 164-171 (2020)

[b-Villar] Villar, A., Lohrmann, A., Bai, X., Vergoossen, T., Bedington, R., Perumangatt, C., Lim, H. Y., Islam, T., Reezwana, A., Tang, Z., Chandrasekara, R., Sachidananda, S., Durak, K., Wildfeuer, C. F., Griffin, D., Oi, D. K. L. and Ling, A. (2020) *Entanglement demonstration on board a nano-satellite*. Optica Vol. 7, Issue 7, pp. 734-737.

[b-Villoresi] Villoresi, P., Jennewein, T., Tamburini, F., Aspelmeyer, M., Bonato, C., Ursin, R., Pernechele, C., Luceri, V., Bianco, G., Zeilinger, A. and Barbieri, C. (2008), *Experimental verification of the feasibility of a quantum channel between space and Earth*, New Journal of Physics Vol. 10, 33038.

[b-Wang-1] Wang, J., Sciarrino, F., Laing, A. and Thompson, M. (2020), *Integrated photonic quantum technologies*, Nature Physics Vol. 14, June, pp. 273-284

[b-Wang-2] Wang, J., Paesani, S., Ding, Y., Santagati, R. Skrzypczyk, P Salavrakos, A, Tura, J., Augusiak, R., Mančinska, L., Bacco, D., Bonneau, D., Silverstone, J., Gong, Q., Acín, A., Rottwitt, K., Oxenløwe, L., O'Brien, L, Laing, A. Thompson, M. (2018), *Multidimensional quantum entanglement with large-scale integrated optics*. Science Vol. 360, April, pp. 285–291.

[b-Wang-3] Wang, Q., Chen, W., Xavier, G., Swillo, M., Zhang, T., Sauge, S., Tengner, M., Han, Z., Guo, G. and Karlsson, A. (2008), *Experimental Decoy-State Quantum Key Distribution with a Sub-Poissionian Heralded Single-Photon Source*. Physical Review Letters Vol. 100, No. 9, March, pp. 090501.

[b-Wang-4] Wang, J., Yang, B., Liao, S., Zhang, L., Shen, Q., Hu, X., Wu, J., Yang, S., Jiang, H., Tang, Y., Zhong, B., Liang, H., Liu, W., Hu, Y., Huang, Y., Qi, B., Ren, J., Pan, G., Yin, J., Jia, J., Chen, Y., Chen, K., Peng, C. and Pan, J. (2013), *Direct and full-scale experimental verifications towards ground–satellite quantum key distribution*. Nature Photonics Vol. 7, April, pp. 387-393.

[b-Wang-5] Wang, C., Yin, Z., Wang, S., Chen, W., Guo, G. and Han, Z. (2017), *Measurement-device-independent quantum key distribution robust against environmental disturbances*. Optica Vol. 4, No. 9, August, pp. 1016-1023.

[b-Wang-6] Wang, S., He, D., Yin, Z., Lu, F., Cui, C., Chen, W., Zhou, Z., Guo, G. and Han, Z. (2019), *Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System*. Physical Review X Vol. 9, No. 2, June, p. 021046.

[b-Wang-7] Wang, S., Yin, Z., Chen, W., He, D., Song, X., Li, H., Zhang, L., Zhou, Z., Guo, G. and Han, Z. (2015), *Experimental demonstration of a quantum key distribution without signal disturbance monitoring*. Nature Photonics Vol. 9, November, pp. 832-836.

[b-Wang-8] Wang, L.-J., Zhang, K.-Y., Wang, J.-Y., Cheng, J., Yang, Y.-H., Tang, S.-B., Yan, D., Tang, Y.-L., Liu, Z., Yu, Y., Zhang, Q., and Pan, J.-W. (2021), *Experimental authentication of quantum key distribution with post-quantum cryptography*. npj Quantum Information Vol. 7, No. 67.

[b-Webinar] Joint ITU-T FG-QIT4N and ETSI webinar (2021), *Opening of the cybersecurity track: Cybersecurity in the quantum era*. https://itu.int/go/QIT-02.

[b-Weedbrook] Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N., Ralph, T., Shapiro, J. and Lloyd, S. (2012), *Gaussian quantum information*. Reviews of Modern Physics Vol. 84, No. 2, May, pp. 621-669.

[b-Wei] Wei, K., Li, W., Tan, H., Li, Y., Min, H., Zhang, W., Li, H., You, L., Wang, Z., Jiang, X., Chen, T., Liao, S., Peng, C., Xu, F. and Pan, J. (2019), *High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics*. Physical Review X Vol. 10, No. 3, August, p. 031030.

[b-Whittaker] Whittaker, Z. (2018), *New plans aim to deploy the first US quantum network from Boston to Washington, DC*. TechCrunch, October 25, 2018. https://techcrunch.com/2018/10/25/new-plans-aim-to-deploy-the-first-u-s-quantum-network-from-boston-to-washington-dc/

[b-Xu] Xu, F., Ma, X., Zhang, Q., Lo, H. and Pan, J (2020), *Secure quantum key distribution with realistic devices*. Reviews of Modern Physics Vol. 92, No. 2, May, pp. 025002.

[b-Yin-1] Yin, J., Li, Y., Liao, S., Yang, M., Cao, Y., Zhang, L., Ren, J., Cai, W., Liu, W., Li, S., Shu, R., Huang, Y., Deng, L., Li, L., Zhang, Q., Liu, N., Chen, Y., Lu, C., Wang, X., Xu, F., Wang, J., Peng, C., Ekert, A. K. and Pan J. (2020) *Entanglement-based secure quantum cryptography over 1120 kilometers*. Nature Vol. 582, June, pp. 501-505.

[b-Yin-2] Yin, J., Cao, Y., Li, Y., Liao, S, Zhang, L., Ren, J., Cai, W., Liu, W., Li, B., Dai, H., Li, G., Lu, Q., Gong, Y., Xu, Y., Li, S., Li, F., Yin, Y., Jiang, Z., Li, M., Jia, J., Ren, G., He, D., Zhou, Y., Zhang, X., Wang, N., Chang, X., Zhu, Z, Liu, N., Chen, Y., Lu, C., Shu, R., Peng, C., Wang, J. and Pan, J. (2017) *Satellite-based entanglement distribution over 1200 kilometers*. Science Vol. 356, No. 6343, June, pp. 1140-1144.

[b-Yin-3] Yin, Z., Han, Z., Chen, W., Xu, F., Wu, Q. and Guo, G. (2008), *Experimental Decoy State Quantum Key Distribution Over 120 km Fibre*. Chinese Physics Letters, Vol. 25, No. 10, October, pp. 3547- 3550.

[b-Yin-4] Yin, H., Chen, T., Yu, Z., Liu, H., You, L., Zhou, Y., Chen, S., Mao, Y., Huang, M., Zhang, W., Chen, H., Li, M., Nolan, D., Zhou, F., Jiang, X., Wang, Z., Zhang, Q., Wang, X. and Pan, J. (2016), *Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fibre*. Physical Review Letters Vol. 117, No. 19, November, p. 190501.

[b-Yu] Yu, Z., Hu, X., Jiang, C., Xu, H. and Wang, X. (2019), *Sending-or-not-sending twin-field quantum key distribution in practice*. Scientific Reports Vol. 9, No. 3080, February.

[b-Yuan-1] Yuan, Z., Plews, A., Takahashi, R., Doi, K., Tam, W., Sharpe, A., Dixon, A., Lavelle, E., Dynes, J., Murakami, A., Kujiraoka, M., Lucamarini, M., Tanizawa, Y., Sato, H. and Shields, A. (2018), *10-Mb/s Quantum Key Distribution*. Journal of Lightwave Technology Vol. 36, No. 16, June, pp. 3427-3433.

[b-Yuan-2] Yuan, Z., Sharpe, A. and Shields, A. (2007), *Unconditionally secure one-way quantum key distribution using decoy pulses.* Applied Physics Letters Vol. 90, pp. 269901.

[b-Yuan-3] Yuan, Z., Dixon, A., Dynes, J., Sharpe, A. and Shields, A. (2009), *Practical gigahertz quantum key distribution based on avalanche photodiodes*. New Journal of Physics, Vol. 11, April, 045019

[b-Zhang] Zhang, Y., Chen, Z., Pirandola, S., Wang, X., Zhou, C., Chu, B., Zhao, Y., Xu, B., Yu, S. and Guo, H. (2020), *Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fibre*. Physical Review Letters Vol. 125, No. 1, June, p. 010502.

[b-Zhao-1] Zhao, Y., Qi, B., Ma, X., Lo, H. and Qian, L. (2006), *Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fibre* in 2006 IEEE International Symposium on Information Theory, July, pp. 2094–2098.

[b-Zhao-2] Zhao, Y., Qi, B., Ma, X., Lo, H. and Qian, L. (2006), *Experimental Quantum Key Distribution with Decoy States*. Physical Review Letters Vol. 96, No. 7, February.

[b-Zhao-3] Zhao, W. (2019), *Development and evaluation of QKD-based secure communication in China*. In ITU Workshop on Quantum Information Technology for Networks, Shanghai, China. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Wenyu_Zhao_Presentation.pdf

[b-Zhong-1] Zhong, X., Hu, J., Curty, M., Qian, L. and Lo, H. (2019), *Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution*. Physical Review Letters Vol. 123, No. 12, September, p.100506.

[b-Zhong-2] Zhong, T., Zhou, H., Horansky, R., Lee, C., Verma, V., Lita, A., Restelli, A., Bienfang, J., Mirin, R., Gerrits, T., Nam, S., Marsili, F., Shaw, M., Zhang, Z., Wang, L., Englund, D., Wornell, G., Shapiro, J. and Wong, F. (2015), *Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding*. New Journal of Physics, Vol. 17, February, p.022002.