Recent Progress in Quantum Key Distribution Network Deployments and Standards

Journal of Physics: Conference Series **2416** (2022) 012001 doi:10.1088/1742-6596/2416/1/012001

Recent Progress in Quantum Key Distribution Network Deployments and Standards

M Stanley, Y Gui, D Unnikrishnan, S.R.G Hall and I Fatadin

National Physical Laboratory, Teddington, United Kingdom

manoj.stanley@npl.co.uk, yunsong.gui@npl.co.uk, divya.unnikrishnan@npl.co.uk, simon.hall@npl.co.uk and irshaad.fatadin@npl.co.uk

manoj.stanley@npl.co.uk

Abstract. Quantum key distribution (QKD) provides in principle unconditional security of key sharing based on the laws of physics only. In the last decade, several experimental and commercial QKD networks have been built and operated worldwide. Demonstrational applications of QKD in financial institutions, government networks, and critical infrastructures such as the power grid have been initially explored. However, large-scale deployment and full-scale commercialization of QKD networks still faces some technological and standardisation challenges. In this paper, recent developments and in-field deployments of QKD networks are reviewed and advancements in QKD standardisation are also discussed.

1. Introduction

The rapid progress of quantum computing technology research and development threatens traditional asymmetric public-key cryptography systems which rely on the computational complexity of prime number factorisation and hence new approaches are required that do not share this vulnerability [1]. Quantum Key Distribution (QKD) is a mechanism for agreeing encryption keys between remote parties, relying on the properties of quantum mechanics to ensure that the key has not been observed or tampered with in transit, which is then used to encrypt information over standard fibre optic links. If the same key is used at both ends of the link the encryption is termed "symmetric". When using QKD there is no reliance on the inability of computers to solve intractable mathematical problems to establish a cryptographic key and the method would be able to resist the advent of high-performance quantum computers. Use cases where QKD 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 and the difficulty of achieving end to-end security. The framework, methods and specification of QKD network test and evaluation, which are crucial for its application and full-scale deployment, are still under development. In this paper, recent large-scale deployments of QKD networks and the programmes under development to overcome these challenges are reviewed. The recent progress in various standardisation activities in QKD research in various Standards Development Organisations (SDO) are also discussed in this paper.

2. Recent progress in QKD

2.1. QKD field deployments and developments

Recently, there has been remarkable progress in the deployment of quantum technologies in communication infrastructures, with several fibre based and free space based QKD networks deployed and under construction worldwide. The discussions in this section are focussed on long range QKD networks deployed within the last 5 years which have been tested and operated over long periods, and therefore, laboratory-scale demonstrations have been excluded from these discussions. QKD deployments before 2018 are summarised in [2] and it is recommended that interested readers refer to this article.

2.1.1. Asia. In China, a large-scale quantum network connecting Beijing, Jinan, Hefei and Shanghai, was constructed consisting of a 2000 km long-distance fibre backbone network containing 700 QKD fibre links interconnected using 32 relay nodes and two satellite–ground links spanning 2600 km [3] as shown in Fig. 1. Different types of topologies were developed to investigate and address wide ranges of parameters such as the trade-offs between cost, security and performance serving more than 150 users. Furthermore, several core techniques were developed, including InGaAs/InP and up-conversion single-photon detectors, dense wavelength-division multiplexing for multiple QKD systems, high-efficiency satellite-ground transmission, real-time post-processing and monitoring, adherence to information security standards, and vitally countermeasures to frustrate existing quantum attacks. The satellite-to-ground QKD in [3] has an average key generation rate of 47.8 kilobits per second, which is 40 times higher than the previous rate [4, 5]. At present, the satellite–ground QKD link does not work during the day and works only when the satellite flies over the ground station, which is at most 4 times a night. The researchers have now also pushed the record for the individual fibre based QKD link without a trusted relay node to beyond 500 km using a new technology known as twin-field QKD (TF-QKD) [6-8]. China plans to build a nationwide QKD network by 2025.

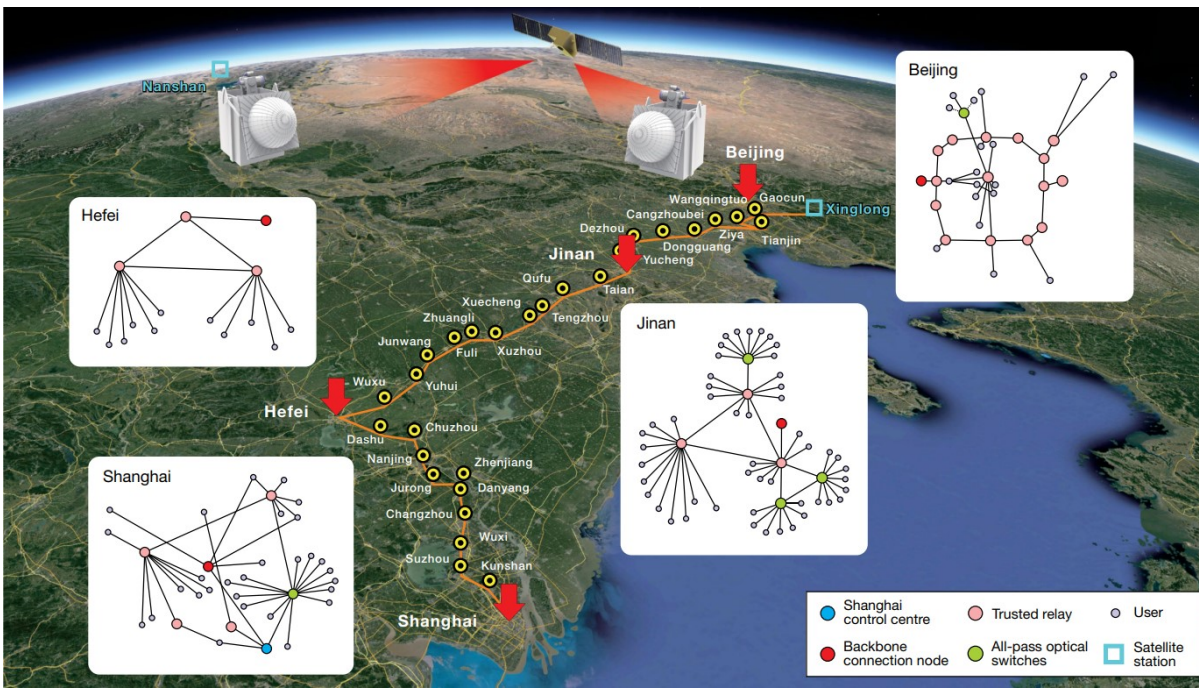

Figure 1. The network consists of four quantum metropolitan-area networks (QMANs) in Beijing, Jinan, Shanghai and Heifei, a backbone fibre link over 2,000 km (orange line) and two ground–satellite links that connect Xinglong and Nanshan (blue squares), separated by 2,600 km. The backbone is connected by trusted relays. A quantum satellite is connected to the Xinglong and Nanshan ground stations; Xinglong is also connected to the Beijing QMAN via fibre [3].

In South Korea, SK Broadband and ID Quantique (IDQ) joined forces to deploy QKD in 17 highly sensitive sites to ensure ultra-secure communications between a network of seven institutions [9]. Toshiba and KT Corporation (KT) will work together to evaluate quality of service (QoS) on a long-distance hybrid QKD network assembled using varied QKD systems, this will take place over an optical fibre network, approximately 490 km long, between Seoul and Busan [10].

In Japan, Nomura HD, Nomura Securities, NICT, Toshiba and NEC engaged in joint verification of the effectiveness and practicality of QKD technology by operating and administering the already established Tokyo QKD network in order to strengthen the security of data communications and storage in the financial sector [11]. The Tokyo QKD network was inaugurated in 2011 and consisted of six optical network links each developed by NTT, NEC, Mitsubishi electric, AIT, IDQ and Toshiba Research Europe [12] as shown in Fig. 2. Recently, Continuous Variable (CV) QKD has been demonstrated to generate a secure key rate of 27.2 kbps with 100 classical traffic channels co-propagating on a 10 km fibre, at 7 dB loss level [13]. In 2020, NEC, NICT, and ZenmuTech encrypted the transmission of electronic medical record samples using QKD and succeeded in backing up samples via a wide area network.

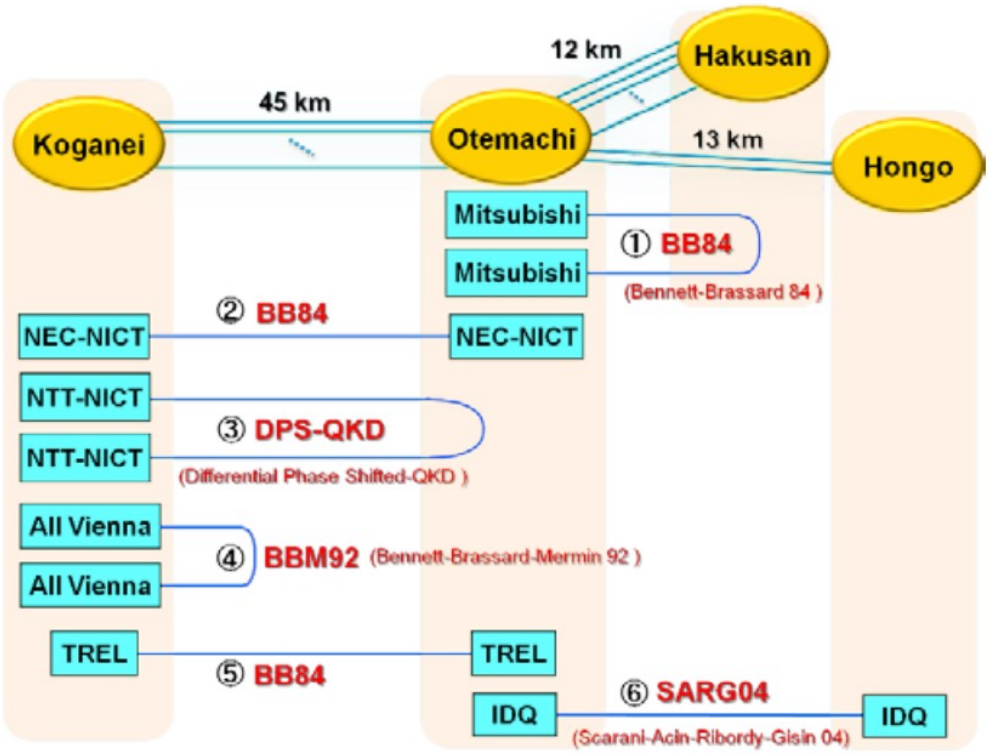

Figure 2. Physical link configuration of the Tokyo QKD Network. It is a mesh-type network consisting of four access points, Koganei, Otemachi, Hakusan, and Hongo with six kinds of QKD systems installed in these access points [12].

In India, a joint team of experts from the Defence Research and Development Organisation (DRDO) and the Indian Institute of Technology (IIT) Delhi recently demonstrated a 100 km fibre based QKD link with key rates up to 10 kbps [14].

2.1.2. Europe. In 2019, the EU launched the Horizon 2020 project OPENQKD. The Austrian Institute of Technology (AIT)-led consortium comprises 38 partners from 9 EU Member States, as well as the UK, Switzerland, Bosnia and Herzegovina, and Israel, consisting of manufacturers, network operators, system integrators, SMEs, research institutions, universities, certification and SDOs, and of course end

users. This was designed to produce a secure quantum communications network in Europe, while also incubating a European ecosystem for quantum technology companies and related application development, the project will focus on developing a variety of demonstrators and future applications. Over the project, 40 QKD systems will be deployed with standardised hardware and software interfaces for network devices and protocols on over 1000 km of fibre links, as well as testing compatibility with satellite-based schemes and 32 use-case trials have already been determined [15]. Some of the use cases include the BerlinaleQ project led by the Fraunhofer Heinrich-Hertz-Institute in Germany for distributing movie data using a highly secure QKD point to point link; QuGenome project led by the University of Aveiro in Portugal to enable a secure multiparty computation service able to perform private recognition of composite signals; Smart Grid project led by SIG Telecom in Switzerland to create a smart grid network and connect 5 power stations to the QKD testbed; high performance computing, banking and healthcare use cases in Poland; academic QKD backbone network in Vienna, etc. UK's National Physical Laboratory (NPL) is the only National Metrology Institute (NMI) involved in OPENQKD and is the main partner in the standardisation work to shape international progress of QKD standardisation and develop framework for certification of QKD.

The "Italian Quantum Backbone" (IQB) developed by the Instituto Nazionale di Ricerca Metrologica (INRiM), in collaboration with the Consiglio Nazionale delle Ricerche (CNR) comprises 1860 km of fibre connecting several cities [2] as shown in Fig. 3. QKD trials on a 40 km dark fibre link within the IQB situated in Florence enabled a secret key rate of ~3.4 kbps and co-existence of quantum and weak classical communication [16]. A QKD link between Sicily and Malta, over ~100 km of dark fibre in an undersea cable with ~30 dB loss and polarisation entanglement based QKD was demonstrated [17]. A QKD enabled video-call between the Italian Prime Minister and the Magnifico Rettore of the Trieste University was demonstrated in 2020. An inter-governmental quantum communication between Italy, Slovenia and Croatia was demonstrated in 2021 through Trieste-Postojna-Ljubljana and Trieste-Rijeka QKD links as part of the EuroQCI initiative during the G20 event held in Trieste as shown in Fig. 4. QKD experiments have been performed on the 100 km Torino-Santhià link where a 30 dB loss has been measured. This link has been extended to 206 km using the Twin Field (TF)-QKD technique [18].

In the UK, a fibre-based quantum network across the south of England linking Cambridge and Bristol, via London and Reading over the National Dark Fibre Infrastructure Service (NDFIS), with extensions to the University of Southampton and the NPL has been setup as shown in Fig. 5. The technology is supplied by ID Quantique, ADVA, BT and Toshiba where Toshiba is testing its QKD prototype based on a single-photon protocol using phase encoding [19]. On the Cambridge-Duxford segment a test running over 3 weeks was made using an aggregated length of 66 km of looped-back fibre with 16 dB link loss. Around 200 Gbps of concurrent classical traffic were encrypted using AES-256 keys provided by a QKD system running over the same fibre in the 1550 nm band with a key rate of 80 kbps [20]. In the section linking the Toshiba Research Europe office (TREL) in Cambridge Science Park to BT's research campus in Martlesham, a standard BT fibre carries both quantum and non-quantum traffic, and 500 Gbps of encrypted data secured by quantum keys are transmitted across a 120 km multiple hop deployed fibre network, with BT exchanges acting as trusted nodes [21]. The Bristol metropolitan area quantum network was formally opened in 2019, with a particular focus on applications of quantum cryptography to 5G telecommunications, because the University of Bristol hosts one of the publicly funded 5GUK test networks [22]. Toshiba partnered with BT to deploy the UK's first industrial deployment of a quantum-secure network over 6 km, transmitting between the National Composites Centre (NCC) in Bristol and the Centre for Modelling & Simulation (CFMS) [23]. In another announcement, the first UK commercial QKD trial is planned by BT and Toshiba, where Ernst & Young (EY) will use the quantum metro network to communicate between two of its sites in London [24]. Funded by the Innovate UK, London based start-up Arqit is building a QKD payload for a satellite to establish the world's first commercial QKD satellite constellation [24]. Arqit, recently announced collaborations with Northrop Grumman and BT to launch two QKD satellites in 2023 from Spaceport Cornwall in the U.K. aboard Virgin Orbit's LauncherOne.

Figure 3. Fibre based Italian quantum backbone network [2].

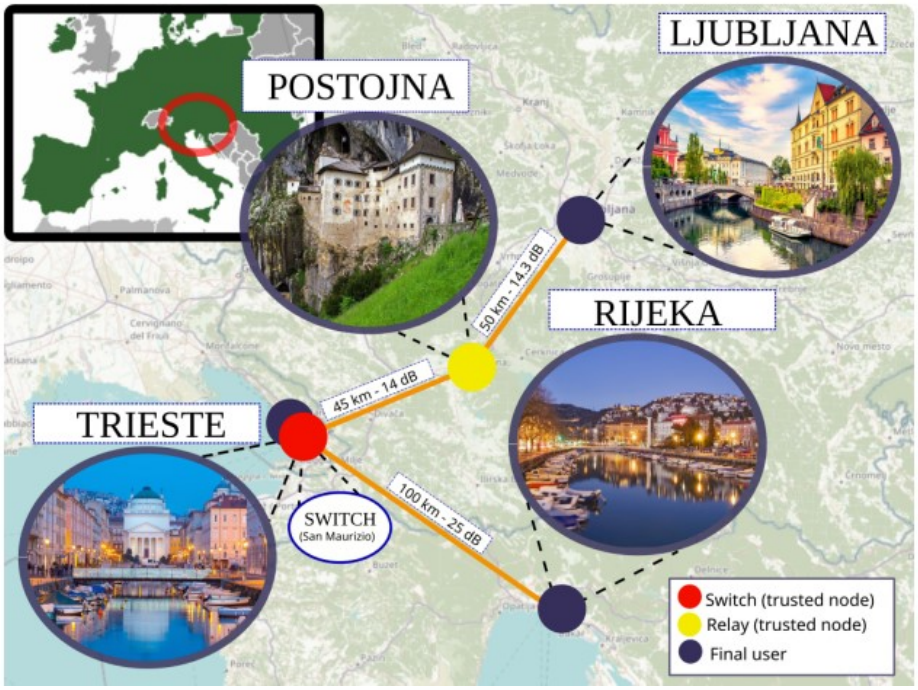

Figure 4. Inter-governmental QKD networks between Italy, Slovenia and Croatia. The network consists of three links and two trusted nodes. The two transmitters (Alices) are in Trieste (Italy) and Ljubljana (Slovenia) while there are two receivers (Bobs) in Postojna (Slovenia) and one in Rijeka (Croatia).

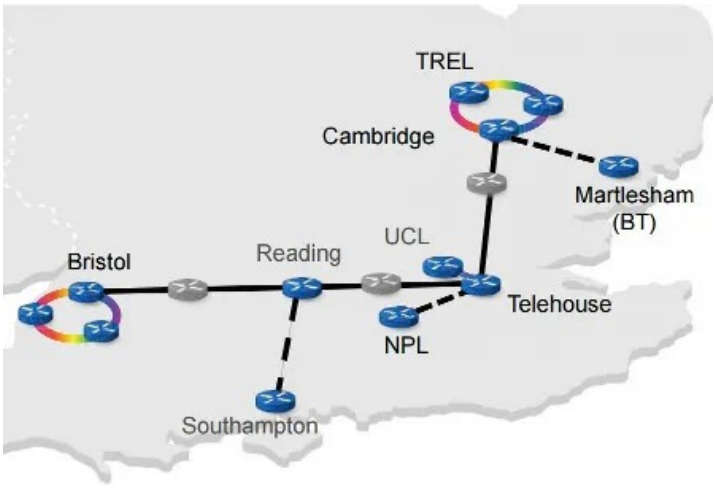

Figure 5. Fibre based UK QKD network [19].

In Spain, Madrid Quantum Communication Infrastructure (MadQCI) as shown in Fig. 6, is an infrastructure that integrates quantum communications in conventional optical networks through Software Defined Networking (SDN) technologies that facilitates the implementation of a flexible, dynamic and scalable network services [26]. It is coordinated by Polytechnic University of Madrid (UPM) in collaboration with Institute IMDEA Software (REDIMadrid) and is part of the European OPENQKD project. The network consists of several dark and lit fibre links to support high and low level Technology Readiness Level (TRL) technology testing. The network also integrates CV-QKD equipment developed by Huawei research laboratories in Munich. The network will run several use cases, such as network security and attestation, critical infrastructure protection, secure cloud services, quantum cryptography for Business to Business (B2B) and 5G networks and self-healed network management [27].

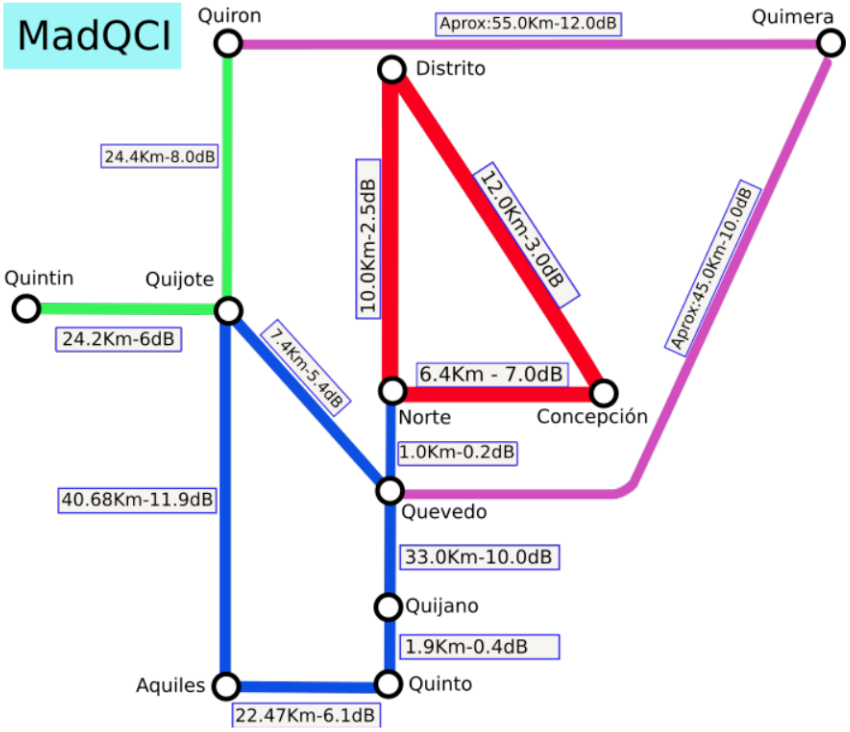

Figure 6. Topology of Madrid Quantum Communication Infrastructure [26].

The Russian Government has released a funding of $0.7 b for development of quantum technologies including creation of quantum network testbeds. This includes setting up secure banking and regional networks in Moscow, backbone QKD networks in St Petersburg, QKD networks with trusted and quantum repeaters in Kazan and a software-defined quantum network in Samara [28]. ITMO University and KRNTU-KAI launched a 160 km intercity quantum channel connecting two cities in Kazan over a deployed fiber in 2019 [29]. QSpace Technologies, a developer of satellite and atmospheric systems in the field of quantum cryptography, will build a small CubeSat with a QKD system transmitter on board and the satellite is scheduled for launch in 2023 [28].

2.1.3. North America. In USA, the National Institute of Standards and Technology (NIST), in coordination with the National Security Agency (NSA), is focused on anointing post-quantum cryptography (PQC) or quantum-resistant mathematical algorithm to be selected as the standard for quantum-based cryptography by releasing a new standard in 2023. Quantum Xchange in collaboration with ID Quantique, launched Phio, which is the first quantum-secured network in the United States. In 2017, the Chinese activism and the results obtained by the Micius satellite led to the enactment of the Quantum National Initiative [30,31]. In this context, NASA has laid out a vision and a roadmap for its quantum activities and few satellite based QKD missions were proposed including QKD from a Mars orbiter to Earth. In 2020, a fibre based QKD network consisting of a pair of connected 26-mile networks between Argonne National Laboratory and Illinois was launched. Recently, a new 35-mile extension was built upon Argonne National Laboratory's network connecting the south side of Chicago [64] to it as shown in Fig. 7. The network is now actively running quantum security protocols using technology provided by Toshiba, distributing quantum keys over fibre-optic cable at a speed of over 80 kbps.

Figure 7. Chicago-Illinois QKD network [64].

In Canada, Honeywell Aerospace in collaboration with University of Waterloo is building the Quantum Encryption and Science Satellite (QEYSSat), on behalf of the Canadian Space Agency [32]. The QEYSSat mission will use a satellite receiver as a trusted node to demonstrate the distribution of secure keys between ground stations separated by at least 400 km and is currently scheduled to be launched into a low-earth orbit in ethe first part of 2024. The QEYSSat mission will utilize both weak coherent pulse sources and entangled photon sources in an uplink configuration to study the performance of QKD, and to perform Bell tests of long-range quantum entanglement.

2.2. QKD standards development

Standards ensure the interoperability of equipment and operating systems from different manufacturers, this allows QT products to be incorporated into existing telecommunication networks. The existence of standards allow confidence in supply chains by defining interfaces and specifications for equipment and distributed systems and their constituent components and modules. One of the benefits of standardisation would be the creation and growth of a market for QKD equipment, as well as avoidance of vendor lock-in towards a specific QKD technology provider. Quantum Key Distribution (QKD) activity by Standards Developing Organisations (SDOs) is currently focussed on fibre based QKD hardware and networks. It is anticipated that this will expand into satellite/free-space hardware and networks in the future.
There are different types of standards, whereby the type of standards being developed often depends on the technological readiness level (TRL) of the innovation. As an example, vocabulary, standards and measurement standards are more likely to be initially developed. As the TRL increases, performance, benchmark or interface standards are more needed. At the end of the innovation, when the product has reached a certain market maturity, interoperability or certification standards will be necessary. The substantial QKD standardisation effort worldwide (with 22 published standards and 20 documents under development) is an indicator of both increased maturity and a strong interest in the practical application and commercialisation of the technology. SDO's have a wide range of standards development activities from terminology to certification standards as discussed in this section.

2.2.1 ETSI. The ETSI Industry Specification Group on Quantum Key Distribution (ISG-QKD, [33]) was the first forum aiming at standardisation of quantum communication technologies. ISG-QKD has produced over 20 documents including general scope documents such as the Vocabulary Group Specification (GS QKD 002, [34]) and Use Cases (GS QKD 007 [35]); technical documents on key extraction from a QKD device (GS QKD 004, [36] and GS QKD 014, [37]) or to control devices (GS QKD 015, [38]); technical documents on QKD security and the exploration of methodologies that real world system imperfections could be used to attack QKD communication systems. (QKD security implementation white paper [39], GS QKD 005, [40], GS QKD 008 [41]) and technical documents on characterization of QKD components (GS QKD 003, [42]) and security proofs and specifications (GS QKD 011, [43]). The current focus is on definition of other interfaces such as network orchestration (GS QKD 018) and authentication (GS QKD 019), that will be needed to create larger secure networks.

2.2.2 ITU-T. ITU standards for QKD networks aim at enabling the integration of QKD technology into large-scale Information and Communications Technology (ICT) networks and provision of the security. The work on QKD networks and security aspects is led by ITU-T Study Group 13 (Future networks and cloud [44]) and ITU-T Study Group 17 ("SG17 Security", [45]). The centrepiece has been the outline of ITU standards for QKD networks, including provision of foundational concepts (ITU Y.3800, [46]), address functional requirements (ITU Y.3801 [47]), architecture (ITU Y.3802, [48]), key management (ITU Y.3803, [49]), control and management (ITU Y.3804, [50]), security framework (ITU X.1710, [51]), key combination methods (ITU X.1714, [52]), and the architecture of a quantum noise random number generator (ITU X.1702, [53]). The Focus Group on Quantum Information Technology for Networks (FG-QIT4N, [54]) was established in September 2019 to provide a collaborative platform for interested stakeholders to take full advantage of the ability and potential of Quantum Key Distribution Networks (QKDN) and Quantum Information Networks (QIN) that are beyond QKDN.

2.2.3 ISO/IEC JTC1. The ISO and IEC in their Joint Technical Committee (JTC1) have quantum technologies standardisation activities with sub-committee SC27 WG3 for security certification of QKD systems. SC27 WG3 [55] has two standards for the security evaluation and certification of QKD systems and develops and maintains the ISO/EN 15408 "Common Criteria for Information Technology Security Evaluation" [56].

2.2.4 CEN-CENELEC. The Focus Group on Quantum Technologies (FGQT) was established by CEN-CENELEC in 2020 to develop a roadmap for standardisation activities related to quantum technology in Europe [57]. The goal is not to directly work on new standards but to identify areas that need to be standardised; start to define a timeline for when standards will be needed, and finally to identify areas where activities could start in the near future.

2.2.5 IEEE. Currently, IEEE is developing two standards which have links to QKD aspects. The P7130 standard is related to specific terminology for quantum technologies, establishing definitions necessary to facilitate clarity and understanding to enable interoperability and compatibility [58]. The P1913 standard defines an application-layer protocol denoted as Software Defined Quantum Communication (SDQC) [59] that communicates over TCP/IP and enables configuration of quantum endpoints in a communication network to actively develop, amend or delete quantum protocols or applications.

2.2.6 CCSA. In China, thriving development of QKD based Quantum Secure Communication (QSC) experimental network construction, demonstrational application, and multi-vendor equipment availability lays a solid foundation for standard research. CCSA-ST7, founded in 2017, has become one of the main promoters of QKD standardization [60]. Two national standard projects including terminology and definition, use cases and requirements, three industry standard projects including QKD system technical requirements, test methods, and a QSC application interface, have been established. The QSC system test and evaluation research project has been completed and released [61]. Other national standard organizations like Cryptography Standardization Technical Committee (CSTC) are also promoting QKD related research.

2.2.7 BSI. The British Standards Institution (BSI), with support from NPL, launched a new panel to bring together interested parties from across the UK quantum technology landscape [62]. This panel will also coordinate, where appropriate, a UK approach to feed into the various international standards development programmes.

2.2.8 Standardisation roadmap. In order to materialise the advantages that standardisation can potentially deliver for the advancement of QKD technology and the transformation into practical applications, the gaps need to be identified and addressed. The missing standards and supplementary documentation and activities need to be prioritised according to their urgency. The QKD standards roadmap [63] in Fig. 8 structures a time plan to this approach.

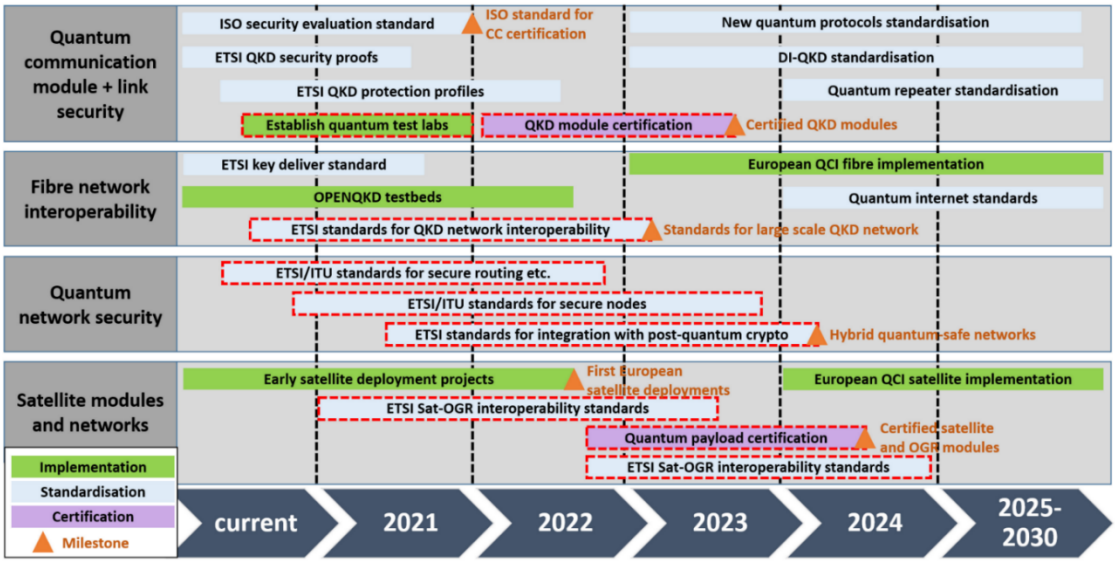

Figure 8. QKD standards roadmap [63].

Activities to drive and support the establishment of the evaluation and certification processes, including involving commercial evaluation laboratories and national certification authorities is underway through European projects such as the OPENQKD. In addition, guidance for the specification and evaluation of particular QKD components, e.g. QKD transmitter and receiver modules, needs to be provided. In the field of security certification of QKD modules, dedicated activities covering almost the entire chain from security specification to evaluation methodology is currently under development in ISO and ETSI, with practically applicable standards expected in early 2022. In the field of QKD networking, gaps exist on two levels: on the level of network interoperability (QKD integration into existing fibre infrastructures, key delivery interfaces, network control, integration of QKD generated keys with cryptographic solutions), and on the level of security certification of networks. Gaps on the networking level are being addressed in ETSI, gaps about the security in networks also have started at ITU-T. A new review of Device Independent (DI) QKD distribution protocols (in draft) is often described as the best methodology for key distribution conducted using "black-box" devices that are uncharacterised. This aims to close loopholes and vulnerabilities identified in "device-dependant" protocols [65]. Development of standards for a future full quantum internet, connecting quantum computers and facilitating the direct transmission of quantum information in a quantum network (including quantum repeaters) will be considered beyond 2025. In the field of satellite modules and networks, early developments are underway but no applicable component and interoperability standards, e.g. for the optical ground receiver, or the satellite optical terminal are available. Standards for the interoperability of space networks and fibre-bound ground networks also still need to be addressed.

3. Conclusion

Currently, organisations such as the National Counterintelligence and Security Center (NCSC) in the US does not endorse the use of QKD, especially in critical infrastructure sectors. Work towards standardising post quantum cryptography (PQC), which can be implemented on today's classical computers and does not require dedicated, or specialist hardware is underway in international standards bodies such as NIST. This is considered a temporary solution as there is a very small possibility that a new algorithm could be developed to break a PQC code in the same way that Shor's algorithm could break the RSA code. However, it is becoming clearer that QKD and PQC can co-exist to provide a complete solution with QKD techniques most appropriate for high security, point-to-point communication links and PQC would be adequate for a broad range of applications for security software. Although, there are few long-range QKD deployments, the vulnerabilities of these networks from various attacks still need to be better understood through standardised benchmarking and testing protocols before utilising QKD networks for critical infrastructure sectors. In addition to technology and standards development, extra efforts must be made to identify and develop applications for real world use to follow the European approach through projects such as OPENQKD for which facilitate widespread Quantum cryptography adoption.

Acknowledgements

This work was supported by the UK government's Department of Business, Energy, and Industrial Strategy (BEIS) through the UK National Quantum Technologies Programme, and Quantum Test and Evaluation programme.

4. References

[1] USA National Security Memorandum/NSM-10, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems", May 4th, 2022
[2] Travagnin M and Miles A L, "Quantum Key Distribution in-field implementations, 2019 European Commission report, EUR 29865 EN.
[3] Chen Y, "An integrated space-to-ground quantum communication network over 4,600 kilometres", 2021 Nature, pp. 214-219.

[4] Liao, S.-K. et al. Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab. Chin. Phys. Lett. 34, 090302 (2017).
[5] Liao, S.-K. et al. Satellite-to-ground quantum key distribution. Nature 549, 43–47 (2017).
[6] Wang S, et.al., "Twin-field quantum key distribution over 830-km fibre", 2022, Nature Photonics, pp. 154-161.
[7] Pittaluga, M. et al. 600-km repeater-like quantum communications with dual-band stabilisation. Nat. Photon. 15, 530–535 (2021).
[8] Jiu-Peng Chen, et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. Nat. Photon. 15, 570-575 (2021).
[9] ID Quantique press release, "IDQ & SK Broadband expand use of QKD to protect critical data in South Korea", 2021, https://www.idquantique.com/id-quantique-and-sk-broadband-expand-the-use-of-quantum-key-distribution-to-protect-critical-information-in-south-korea/
[10] Toshiba Digital solution press release, "Toshiba Group and KT Collaborate on Quantum Key Distribution Pilot Projects in South Korea", 2022, https://www.global.toshiba/ww/company/digitalsolution/news/2022/0328.html#id03
[11] NICT press release, "Beginning Joint Verification Tests on quantum cryptography technology to enhance cybersecurity in the financial sector", 2021, https://www.nict.go.jp/en/press/2021/01/18-1.html
[12] M. Sasaki, "Field test of quantum key distribution in the Tokyo QKD Network", Optics express, 10387, vol. 19, 2010.
[13] "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3Tbit/s data channels", Communications Physics, Vol. 2, 9, 2019,
[14] Ministry of defence Government of India, "DRDO and IIT Delhi scientists demonstrate Quantum Key Distribution between two cities 100 kilometres apart", 2022, https://pib.gov.in/PressReleasePage.aspx?PRID=1800648
[15] Open QKD, 2020, https://openqkd.eu/openqkd-in-action/
[16] Davide Bacco, "Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area", EPJ Quantum Technology volume 6, Article number: 5 (2019)
[17] Wengerowsky S, "Entanglement distribution over a 96-km-long submarine optical fiber", Proc Natl Acad Sci USA. 2019, 116(14): 6684–6688.
[18] Cecilia Clivati, "Coherent phase transfer for real-world twin-field quantum key distribution", Nature Communications, 13, Article number: 157 (2022).
[19] Technical specifications available on the Toshiba website https://www.toshiba.eu/eu/Cambridge-ResearchLaboratory/ Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/
[20] "Field trial of a QKD and High-Speed Classical Data Hybrid Metropolitan Network", Proc. SPIE 10559, Broadband Access Communication Technologies XII, 1055907, 2018.
[21] "Field trial of a QKD and high-speed classical data hybrid metropolitan network", Photonics West, San Francisco, 2018.
[22] https://www.bristol.ac.uk/physics/research/quantum/conferences/qkdover5guk/
[23] BT press release, "BT and Toshiba install UK's first quantum-secure industrial network between key UK smart production facilities", 2020.
[24] Ernst & Young press release, "BT and Toshiba launch first commercial trial of quantum secured communication services – EY becomes first commercial customer", 2022.
[25] UKRI, "Next Generation Satellite QKD - Creating a UK Sovereign Capability for Manufacturing Satellite QKD Payloads", 2020.
[26] D. Lopez, "Madrid Quantum Communication Infrastructure: a testbed for assessing QKD technologies into real production networks", Optical Fiber Communications Conference and Exhibition, San Francisco, 2021.
[27] V. Martin, "The Madrid SDN Quantum Network", ITU Workshop on Quantum Information Technology for Networks, Shanghai, 2019.
[28] V. Egorov, "Quantum communication in Russia: status and perspective", Shanghai, 2019.
[29] Kozubov, Anton, Andrei Gaidash, and George Miroshnichenko. arXiv preprint arXiv:1903.04371 (2019).

[30] "Chinese Efforts in Quantum Information Science: Drivers, Milestones, and Strategic Implications", Testimony for the U.S.-China Economic and Security Review Commission, March 16th, 2017 https://www.uscc.gov/sites/default/files /John%20Costello_Written%20Testimony_Final2.pdf
[31] "The U.S. National Quantum Initiative: From Act to action", Science, Vol. 364, Is. 6439, pp. 440-442, 2019 https://science.sciencemag.org/content/364/6439/440. See also https://scipol.org/track/hr-6227-nationalquantum-initiative-act/national-quantum-initiative-act-public-law-115-368
[32] Podmore, H., "QKD terminal for Canada's Quantum Encryption and Science Satellite (QEYSSat)", Proc. SPIE 11852, International Conference on Space Optics, Jun 2021.
[33] ETSI, "Industry specification group (ISG) on quantum key distribution for users (qkd)", https://www.etsi.org/committee/1430-qkd
[34] ETSI GS QKD 002, "Quantum Key Distribution; Use Cases", https://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/ 01.01.01_60/gs_qkd002v010101p.pdf, June 2010.
[35] ETSI GR QKD 007, "Quantum Key Distribution (QKD); Vocabulary", https://www.etsi.org/deliver/etsi_gr/QKD/ 001_099/007/01.01.01_60/gr_qkd007v010101p.pdf, December 2018.
[36] ETSI GS QKD 004, "Quantum Key Distribution (QKD); Application Interface", https://www.etsi.org/deliver/etsi_gs/ QKD/ 001_099/004/02.01.01_60/gs_qkd004v020101p.pdf, August 2020.
[37] ETSI GS QKD 014, "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API", https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf, February 2019.
[38] ETSI GS QKD 015, "Quantum Key Distribution (QKD); Control Interface for Software Defined Networks", https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/01.01.01_60/gs_QKD015v010101p.pdf , March 2021.
[39] Marco Lucamarini, et.al., "Implementation Security of Quantum Cryptography Introduction, challenges, solutions", ETSI White Paper No. 27, ISBN No. 979-10-92620-21-4, https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf, July 2018.
[40] ETSI GS QKD 005, "Quantum Key Distribution (QKD); Security Proofs", https://www.etsi.org/deliver/etsi_gs/qkd/ 001_099/005/01.01.01_60/gs_qkd005v010101p.pdf, December 2010.
[41] ETSI GS QKD 008, "Quantum Key Distribution (QKD); QKD Module Security Specification", https://www.etsi.org/ deliver/etsi_gs/qkd/001_099/008/01.01.01_60/gs_qkd008v010101p.pdf, December 2010
[42] ETSI GR QKD 003, "Quantum Key Distribution (QKD); Components and Internal Interfaces", https://www.etsi.org/ deliver/etsi_gr/QKD/001_099/003/02.01.01_60/gr_qkd003v020101p.pdf, March 2018.
[43] ETSI GS QKD 011, "Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems", https://www.etsi.org/deliver/etsi_gs/qkd/ 001_099/011/01.01.01_60/gs_qkd011v010101p.pdf, May 2016.
[44] ITU-T Study Group 13, "Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructure", https://www.itu.int/en/ITUT/about/groups/ Pages/sg13.aspx
[45] ITU-T Study Group 17, "Security", https://www.itu.int/ en/ITUT/about/groups/Pages/sg17.aspx
[46] ITU-T Y.3800, "Overview on networks supporting quantum key distribution", https://www.itu.int/itu-t/ recommendations/rec.aspx?rec=13990, October 2019.
[47] ITU-T Y.3801, "Functional requirements for quantum key distribution networks", https://www.itu.int/itu-t/ recommendations/ rec.aspx?rec=14258, April 2020.

[48] ITU-T Y.3802,, "Quantum key distribution networks – Functional architecture", https://www.itu.int/itu-t/ recommendations/rec.aspx?rec=14407, December 2020.
[49] ITU-T Y.3803 (12/2020), "Quantum key distribution networks – Key management", https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14408, December 2020.
[50] ITU-T Y.3804, "Quantum key distribution networks – Control and management", https://www.itu.int/itu-t/ recommendations/rec.aspx?rec=14409, September 2020.
[51] ITU-T X.1710 (10/2020), "Security framework for quantum key distribution networks", https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14452, October 2020.
[52] ITU-T X.1714 (10/2020), "Key combination and confidential key supply for quantum key distribution networks", https://www.itu.int/itut/recommendations/rec.aspx?rec=14453, October 2020.
[53] ITU-T X.1702 (11/2019), "Quantum noise random number generator architecture", https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14095, November 2019.
[54] ITU-T Focus Group on Quantum Information Technology for Networks (FGQIT4N), https://www.itu.int/en/ITU-T/ focusgroups/qit4n/Pages/default.aspx
[55] ISO/IEC JTC 1/SC 27/WG 3, "Security evaluation, testing and specification, https://standards.iteh.ai/catalog/ tc/iso/56ffc1fc-b504-40a6-b4ab-3cacf8ff9f7d/iso-iec-jtc-1-sc-27-wg-3
[56] NEN-EN-ISO/IEC 15408-1, "Evaluation criteria for IT security - Part 1: Introduction and general model", https://www.nen.nl/nen-en-iso-iec-15408-1-2020-en269562, 2020.
[57] CEN-CENELEC Focus Group on Quantum Technologies, FGQT, https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/
[58] IEEE P7130, "Standard for Quantum Technologies Definitions", https://standards.ieee.org/project/7130.html
[59] IEEE P1913, "Software-Defined Quantum Communication", https://standards.ieee.org/project/1913.html
[60] Lai J, et.al, Test evaluation and standardization progress of QKD based quantum secure communication", 2018 Asia Communications and Photonics Conference (ACP).
[61] CCSA-ST7, " Quantum communication and information technology," http://www.ccsa.org.cn/tc/index.php?tcid=st7
[62] BSI, "New ICT/1/1/2 quantum technology panel", https://www.bsigroup.com/en-GB/industries-and-sectors/ quantum-technology/.
[63] M. Loeffler, et.al, "Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution", OPENQKD report, 2021.
[64] University of Chicago press release, "Chicago expands and activates quantum network, taking steps toward a secure quantum internet", 2022,
[65] Primaatmaja, I.W., Goh, K.T., Tan, E.Y.Z., Khoo, J.T.F., Ghorai, S. and Lim, C.C.W., 2022. Security of device-independent quantum key distribution protocols: a review. arXiv preprint arXiv:2206.04960.