JRC TECHNICAL REPORTS

Quantum Key Distribution in-field implementations

Technology assessment of QKD deployments

Travagnin, Martino
Lewis, Adam, M.

2019

Joint Research Centre

EUR 29865 EN

Contact information
Name: Adam M. Lewis
Address: Centro Comune di Ricerca, Via E. Fermi 2749, I-21027 Ispra (VA) ITALY
Email: adam.lewis@ec.europa.eu
Tel.: +39 0332 785786

EU Science Hub
https://ec.europa.eu/jrc

JRC118150

EUR 29865 EN

PDF ISBN 978-92-76-11444-4 ISSN 1831-9424 doi:10.2760/38407

Luxembourg: Publications Office of the European Union, 2019

How to cite this report: Travagnin, Martino and Lewis, Adam, M., "Quantum Key Distribution in-field implementations: technology assessment of QKD deployments", EUR 29865 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11444-4, doi:10.2760/38407, JRC118150

Contents

Abstract

This report briefly describes quantum key distribution field deployments worldwide. It updates the material presented in the JRC science for policy report EUR 29017 of 2017, and adds some technical details. Both terrestrial and satellite deployments are included, and both publicly funded and privately funded initiatives. The report forms part of a study to define a vision for a European quantum communications infrastructure, and its focus is on technology demonstrated in a relevant environment: theoretical work, laboratory-scale experimental research, and one-off, small-scale field pilots are therefore not covered.

Acknowledgements

This work is part of JRC Work Package 6315 and was funded by the European Commission's Directorate-General for Communications Networks, Content and Technology, under Administrative Arrangement No. 35420-2019 with the JRC.

Authors

Martino Travagnin

Adam M. Lewis

Executive summary

Quantum-based techniques for communications security are slowly emerging as a complement to algorithmic and non-quantum physical layer methods. 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 and the difficulty of achieving end-to-end security. Intensive public research and development funding is being applied worldwide to overcome these difficulties, and several testbeds have now been deployed which are here surveyed. As a general rule, we have restricted the survey to networks of at least kilometre scale which have been operated over periods of at least several days, and we have excluded laboratory-scale demonstrations and brief scientific experiments over longer distances.

Worldwide, a significant amount of experience with quantum communication deployments has already been acquired. Some of the deployments use hardware made in academic facilities but many employ equipment from companies such as QuantumCTek, China Quantum Technologies, ID Quantique, Toshiba and Huawei.

The largest single network is in China, with a 2 000 km long backbone from Shanghai to Peking, with metropolitan networks in these cities and in Heifei and Jinan. Smaller deployments have also been made in Korea and in Japan, specifically in Tokyo. The Chinese and Japanese approaches reveal different priorities. In China, a large network has been built very quickly with technology which is ready now, whereas in Japan, work has focused on systematically evaluating the developing technology variants against use cases. Both countries have experimented with QKD in low earth orbit (LEO) satellites. A dedicated satellite was launched by China, to demonstrate the feasibility of several QKD prepare-and-measure and entanglement-based protocols; Japan has conducted a small-scale experiment on a non-dedicated satellite-mounted optical terminal, demonstrating that quantum communications with a quantum bit error rate low enough to enable QKD are possible, even with a microsatellite.

In the EU, 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. The main importance of this work is that it showed the interoperability of different types of QKD system in a trusted node network. The largest fibre deployment in Europe is in Italy, with a network now extending almost the entire length of the peninsula from Turin to Milan and Matera. This is mostly based on commercial equipment and dark fibre, with some university-built hardware in a metro network in Florence. QKD experiments have actually been done only in some spans of the network; efforts to foster some take-up by prospective users are underway. The quantum communications network is used with separate in-fibre distribution of precise time from the INRiM metrology laboratory in Turin, enabling quantum-based assurance of a time stamp e.g. for financial transactions. Experiments have also been conducted with distribution via undersea fibre to Malta and passive reflection from LEO satellites of quantum signals sent from the Italian Space Agency's Matera ground station. The first long term network both in Europe and worldwide was the SwissQuantum project, operating from March 2009 to January 2011, focused on performance, flexibility and reliability. The network included key management and application layers, as well as the quantum layer itself.

In Russia, test networks have been deployed in Moscow and St Petersburg. The Moscow work has focused on applications, especially in banking. The testbed in St Petersburg has been used to test a novel high speed protocol. A metropolitan network in Madrid has been used to develop concepts for employing QKD in software defined telecommunication networks (SDN), the emphasis being on full integration with the network, rather than on high speed or long distance, the concept being protection of the network as well as QKD as a service. A network now under construction in the UK will incorporate both long distance and telecommunication network integration. Metropolitan networks in Cambridge and Bristol are now operational and the link from Cambridge to London is under test. The Cambridge local area network extends to BT's laboratories near Ipswich and notably has been used 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. Plans for future projects have also been made public elsewhere in Europe. The nearest to deployment appears to be in Poland where there is well-developed scheme for a network in the Wrocław area.

In the USA, fibre-based and free-space experiments were made as early as 2004 in the Boston area. Relatively little activity took place subsequently in the USA until the private Batelle organisation deployed a system in Ohio in 2013. In 2019, the Quantum Xchange company 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 US has recently launched a national quantum programme within which 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 27km, using commercial equipment in dark fibre.

A number of QKD protocols have been used in the above deployments. The best established and most widely used have been with single photon protocols of the BB84 and related types but coherent one way and continuous variable QKD have also been deployed at scale. Also in the majority are deployments in which the quantum channel is in dark fibre, although several examples are known of quantum channels multiplexed with classical data in the same fibre. While some deployments of measurement-device-independent QKD are being done, very few attempts have been made to make use of other forms of entanglement-based QKD, which is clearly at a lower level of technology readiness.

Whatever QKD scheme is used, the secure key rate achieved depends on the link distances and losses, protocol, hardware and whether or not dark fibre is used. But it also depends on how the system is configured, according to the amount of information leakage deemed acceptable, so comparing the performance of different deployments requires some care. We have attempted to do so, focusing on the distances and secure key rate as the parameters of most importance to potential users.

1 Introduction

The dependence of modern civilizations on secure information exchange makes cybersecurity a priority for governments across the world, the EU included. Quantum communications is an emerging technology with potential to aid significantly in maintaining information security, especially in the event that present-day asymmetric cryptography schemes were compromised. Quantum key distribution (QKD) is the most technologically mature application of quantum communications, and is already available commercially from some vendors. However, 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, have greatly slowed uptake and relegated application to niche cases. A growing and energetic QKD research community seeks ways to break through the technical bottlenecks. In the EU this especially includes projects financed through the Quantum Technologies Flagship, and the accompanying QuantEra, COST and EuraMet programmes, as well as projects funded by member states. It is therefore expected that several other QKD in-field experiments will be performed in the near future, and some countries are known to be extending their deployments or planning new testbeds. The European Commission is already actively pursuing the vision of a quantum communications infrastructure (QCI) for Europe. It is expected that work on a QKD testbed will begin this year. The case for scaling up to an operational network requires a clear rationale based on use cases and associated architectures, and a technology roadmap.

This present report contributes to the QCI discussions by surveying the current status of field deployment of quantum key distribution, adding some technical details to the survey contained in the JRC report EUR 29017 EN "The impact of quantum technologies on the EU's future policies - quantum communications: from science to policies", 2018, to which the reader is referred for background information.

2 Asia

2.1 China

The Beijing-Shanghai quantum backbone is now operational. It is ~2 000 km long, and relies on 32 trusted nodes. The quantum channel makes use of a dedicated ("dark") fibre at 1550 nm and prepare-and-measure discrete QKD protocols are employed; the all-pass secure key rate is thought to be in the ~20-30 kbps range, although official figures have not been released[1]. Several users have been reported (see Fig. 1), but it is difficult to assess how much the infrastructure is actually employed to address concrete needs. Many use cases have been elaborated by the commercial vendor QuantumCTek, which provided the QKD hardware for some spans and tested additional equipment optimized for applications in critical infrastructure protection[2].

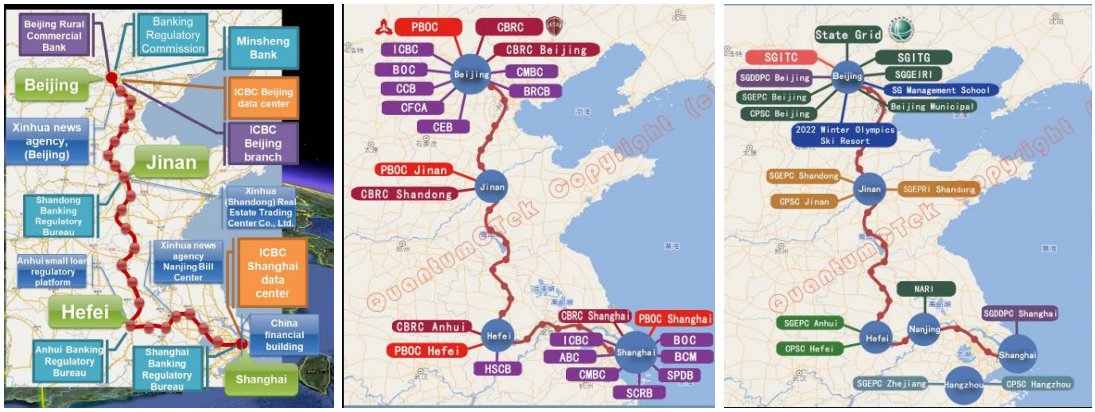


Fig. 1: users of the quantum backbone: main players (left), banks (centre), and power grid operators (right).

For an average fibre span of 70 km, estimating a fibre loss of 0.2 dB/km with a 30% increase due to deployment, we have a typical loss per span of ~18 dB. This number is consistent with the specs provided by QuantumCtek: the commercial QKD-PHA300 and QKD-POL1250 racks declare a typical secret key rate of 50 kbps and 80 kbps respectively in a 10 dB-loss channel, and 1 kbps at a loss level of 22 dB and 24 dB respectively.

Another commercial provider of quantum communications equipment is China Quantum Technologies (QTEC), with which in December 2016 the Swiss firm ID Quantique announced the creation of a joint venture to bring its Quantum Random Number Generators (QRNGs) and Quantum Key Distribution (QKD) solutions to the Chinese market[3]. A third commercial provider is Anhui Qasky Quantum Technology (Qasky), which sold some of the hardware deployed in China's quantum networks[4].

The first large-scale quantum network deployed in China for which a complete technical description is available was deployed in the Hefei-Chaohu-Wuhu area on a China Mobile infrastructure consisting mainly of standard ITUT G.652 fibres, see Fig. 2. Dark fibres

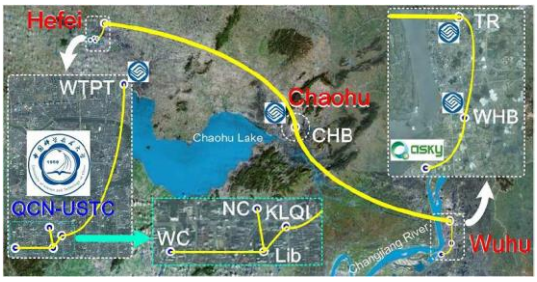
[1] "Large scale quantum key distribution: challenges and solutions", Optics Express Vol. 26, No. 18 (2018) https://www.osapublishing.org/DirectPDFAccess/F53E7827-CFE2-3D07-9B8528A9C8AAE9AE_396720/oe-26-18-24260.pdf?da=1&id=396720&seq=0&mobile=no

[2] http://www.quantum-info.com/English/

[3] https://www.idquantique.com/idq-qtec/

[4] http://www.qasky.com/EN

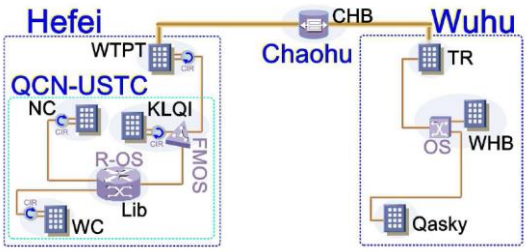
were used to transmit the quantum and the synchronization signals in the 1 550 nm band. The wide area network had over 150 km of coverage area: the Hefei metropolitan area QKD network offered all-to-all interconnections, while the Wuhu area QKD network had a point-to-multipoint configuration[5].



	Optical fiber link	Length of fiber(km)	Optical loss(dB)
Hefei metro network	WTPT–USCT(KLQI)	16.9	−6.1
	KLQI–Lib	0.9	−1.2
QCN–USTC	NC–Lib	1.2	−0.6
	WC–Lib	1.9	−0.5
HCW-intercity link	Hefei–Chaohu	85.1	−18.4
	Chaohu–Wuhu	69.7	−14.1
Wuhu metro network	TR–WHB	14.3	−5.0
	WHB–Qasky	9.0	−7.1

Fig. 2: Layout of the network and distances between the nodes, with the relative optical losses

The whole network was tested for more than 5 000 hours, from December 2011 to July 2012. Through standardised design of QKD devices and seamless dynamical switching, an effective integration between point-to-point QKD techniques and networking schemes was realised. A total of 13 QKD devices were deployed, implementing the decoy-state phase-coding BB84 protocol, and ensuring the long-term performance shown in Fig. 3.



	QKD link	QKD devices	Secure key rate(kbps)
Hefei metro network	KLQI→NC	T1→R3	7.27
	NC→WC	T3→R4	8.33
	WC→KLQI	T4→R1	6.86
	WTPT→NC	T2→R3	1.05
	NC→WC	T3→R4	8.33
	WC→WTPT	T4→R2	1.02
	KLQI→WTPT	T1→R2	2.67
	WTPT→KLQI	T2→R1	2.42
	NC→WC	T3→R4	13.39
	WC→NC	T4→R3	16.15
HCW-intercity link	Hefei→Chaohu	T5→R5	0.77
	Chaohu→Wuhu	T6→R6	0.80
Wuhu metro network	WHB→TR	T7→R7	6.07
	Qasky→TR	T8→R7	0.96

Fig. 3: Overall topology and performances along the links connecting the nodes. Abbreviations in black and blue are locations, abbreviations in grey are optical components - CIR: optical circulator, OS: optical switch, FMOS: full-mesh optical switch, R-OS: router and optical switch combination.

Large scale metropolitan quantum networks have since been deployed in Beijing, Shanghai, Hefei (46 nodes), Jinan (56 nodes). From an article published by the China Daily on 11 July 2017, we read: "Jinan, capital of Shandong province China, will become the first city in the world, by the end of August, to use ultra-secure quantum communication in government. The network, which cost 120 million yuan ($19.5 million), will connect Party and government offices. The system has passed more than 50 rounds of tests since May and is capable of encrypting more than 4 000 pieces of data every second and transmitting information to 200 terminals in the city. The first users of this technology will be government agencies, the military, finance, and electricity sectors"[6].

[5] "Field and long-term demonstration of a wide area quantum key distribution network", Optics Express, Vol. 22, Issue 18, pp. 21739-21756 (2014), https://arxiv.org/pdf/1409.1568.pdf

[6] "Quantum tech to link Jinan governments", China Daily, 11 July 2017
http://www.chinadaily.com.cn/china/2017-07/11/content_30065215.htm

In other deployments "lit" fibre has been used, i.e. with the quantum channel multiplexed with classical traffic, allowing for lower installation costs at the price of slower key rate and/or shorter span length. Using the telecom window at ~1 300 nm for the quantum channel, ~3.0 kbps of secure key over 66 km of deployed standard fibre have been demonstrated along the Jinan-Qingdao backbone, with 3.6 Tbps of concurrent classical traffic at ~1 550 nm[7]. The quantum channel coexists with classical ones also in parts of the Wuhan metropolitan quantum network.

In addition to discrete QKD (which guarantees the best performance, but requires expensive single-photon detectors), continuous-variable quantum key distribution (CV-QKD) has also been used in China in real-word deployments. CV-QKD has been deployed in the Shanghai university campuses, with quantum signal and classical wavelength division multiplexed (WDM) traffic both travelling in the ~1 550 nm band: 5 different links have been tested, with lengths ranging between ~2 km and ~40 km. As the loss increases from ~3 dB to ~15 dB, the secret key rate decreases from 10 kbps to 0.25 kbps[8]. A commercial vendor of CV-QKD equipment is XTQuantech, established in March 2017[9]. In May 2019 an experiment was reported in which CV-QKD was performed over two commercial deployed dark fibres, respectively in Xi'an and Guangzhou: over a ~30 km fibre with 12.48 dB loss a secure key rate of 5.91 kbps was achieved, while over a ~50 km fibre with ~11.62 dB loss the secure key rate was 5.77 kbps[10].

Tests in real-world deployments have been made also for measurement-device-independent (MDI) QKD, which features enhanced resistance against eavesdropping attacks targeting the detectors. Such technology however still presents significant technical challenges, and yields low key rates even when high-cost superconducting nanowire single photon detectors are employed. In Hefei, a 4 node star topology has been implemented: for three fibre spans with lengths of 17 km (5.1 dB loss), 25 km (9.2 dB loss) and 30 km (8.1dB loss) the secure key rates were 38.8 bps, 29.1 bps, and 16.5 bps respectively[11].

Coming to space-based QKD, the Micius satellite (weight 640 kg, power 560 W, 300 mm and 180 mm telescopes on-board) was launched in August 2016 and is now operational. Single photons are emitted at 850 nm with a repetition rate of 100 MHz. During a pass of duration ~270 s, the sifted key rate decreases from ~12 kbps at 650 km to ~1 kbps at 1200 km, when a 1 m telescope on the ground is used as the receiving end. After error correction and privacy amplification ~300 kb of secure key are obtained, corresponding to a key rate of ~1.1 kbps[12].

---

[7] "Integrating QKD with classical communications in backbone fiber network", Optics Express Vol. 26, 5, 2018 https://arxiv.org/abs/1709.10046#

[8] "Field demonstration of a continuous-variable QKD network", Optics Letters, Vol. 41, No. 15, 2016 https://www.researchgate.net/publication/305620355_Field_demonstration_of_a_continuous-variable_quantum_key_distribution_network

[9] http://www.xtquantech.com/en/about/

[10] "Continuous-variable QKD over 50km commercial fiber", 2019 https://arxiv.org/abs/1709.04618

[11] "Measurement-Device-Independent QKD over untrustful metropolitan network", Phys. Rev. X 6, 011024, 2016, https://journals.aps.org/prx/pdf/10.1103/PhysRevX.6.011024

[12] "Satellite-to-ground quantum key distribution", Nature, Vol. 547, pg. 46, 2017 https://www.nature.com/articles/nature23655.pdf

Also, the Tiangong-2 space laboratory has been used to perform a space to ground QKD experiment, by using a 58 kg payload with a 200 mm telescope: a key rate of ~0.1 kbps at a distance of up to 719 km was demonstrated[13].

The Micius satellite has been used as a trusted node for intercontinental QKD between China and Europe, linking two locations at a distance of 7600 km. The key (which was also transmitted along a 280 km optical ground connection between Xinglong and Beijing) was used to one-time-pad (OTP) encrypt two ~5 kByte pictures and to AES-encrypt a video conference, refreshing the 128-bit seed key every second[14]. Entanglement distribution has also been demonstrated, using an entanglement source generating 5.9 million entangled photon pairs per second at 810 nm. At two receiving ground stations separated by ~1200 km, the averaged received entangled two-photon count rate is 1.1 Hz[15]. Quantum teleportation in uplink configuration has also been performed[16].

A considerable extension of the terrestrial QKD network is planned, as shown in Fig. 4: part of the infrastructure will also be used for time and frequency transfer. Talks about further quantum satellites, also in MEO and GEO orbits, are common, but no details have been made available.

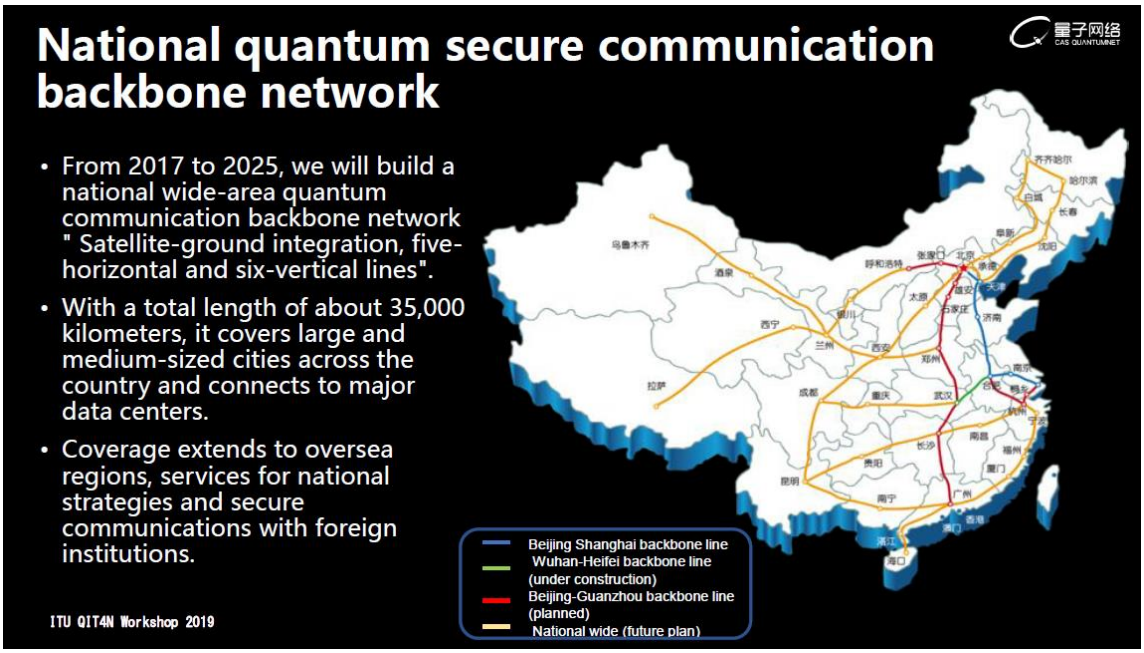


Fig. 4: actual deployments and plans for further extension of the terrestrial QKD network in China

[13] "Space-to-Ground Quantum Key Distribution Using a Small-Sized Payload on Tiangong-2 Space Lab", Chinese Physics Letters, Volume 34, Number 9, 2017, https://iopscience.iop.org/article/10.1088/0256-307X/34/9/090302

[14] "Satellite-Relayed Intercontinental Quantum Network", Phys. Rev. Lett. 120, 030501, 2018 https://arxiv.org/ftp/arxiv/papers/1801/1801.04418.pdf

[15] "Satellite-based entanglement distribution over 1200 kilometers", Science, Vol. 356, Issue 6343, pp. 1140-1144, 2017, https://science.sciencemag.org/content/356/6343/1140

[16] "Ground-to-satellite quantum teleportation", Nature, Vol. 547, pg. 70, 2017 https://www.nature.com/articles/nature23675

2.2 **Japan**

Work on a QKD testbed in Tokyo started ~10 years ago: since the beginning, the project was aimed not only at technology testing but also at verifying its practical uses. The importance of information-theoretically secure encryption with one-time-pad is emphasized: one of the aims of the project was to increase the typical QKD link performance in real-world deployments from a secure key rate of a few kbps on few tens of km (sufficient to encrypt voice data by real-time OTP or to feed the primary session key to a classical encryptor) to performance level high enough to enable OTP encryption of video over tens of km. In 2010 the UQCC (Updating Quantum Cryptography and Communications) website wrote that "after sufficient tests of long-term operation stability in the Tokyo QKD Network, QKD systems are expected to be deployed first in the NICT internal networks. They will then be installed into government agencies networks and mission critical infrastructures where communication security is imperative to protect state secrets. Further improvements in device compactness will then expand the application area of QKD to financial, medical and business organizations for the well-being of the public"[17].

As shown in Fig. 5, the testbed includes 6 nodes linked by commercial fibres. The loss rate is in the 0.3-0.5 dB/km range, and the percentage of aerial cables is about 50%, which increases susceptibility to environmental fluctuation. Different QKD protocols and implementations have been tested by several developers, with varying performance levels. Here a brief summary of the main results[18]:

- NEC-NICT: 45 km, 14.5 dB channel loss, multi-channel QKD at 1 550 nm. Secure key rate ~80 kbps on a single channel, usable for video OTP encryption. The block size was 750 kbits, but it was acknowledged that "this size may need to be longer" to avoid finite-size effects which can compromise the security of the key.
- TREL: 45 km, 14.5 dB channel loss, 1 GHz modulation, InGaAs single photon detectors electrically cooled −30°C and gated. Secure key rate ~300 kbps, usable for video OTP encryption.
- NTT-NICT: 90 km, 27 dB channel loss. Secure key rate ~2.1 kbps, for voice OTP encryption in real time.
- Mitsubishi: 24 km link with a total loss of 13 dB, using InGaAs/InP avalanche photodiodes cooled down to −40°C. The secure key rate is 2 kbps, obtained on blocks of distilled key of 10^6 bits, "which is currently known to be the minimum block size to eliminate the finite size effect". Mitsubishi also developed an OTP smartphone using QKD, to provide end-to-end encryption of voice data between smartphones. A secure key is downloaded from QKD apparatus to the smartphone, and voice is encoded with a rate of 1 kB per second, requiring ~1.2 MB for a 10 min bidirectional talk. By using a 2 GB Secure Digital (SD) card, continuous conversation for 10 days by OTP encryption can be supported with a single downloading.
- ID Quantique: reliable and highly stable long term operations of the commercial quantum key distribution Cerberis apparatus on a 13 km link with 11 dB loss, demonstrating a secure key rate of ~0.3-0.4 kbps. In the brochure now distributed by ID Quantique for Cerberis it is stated that at the maximum transmission loss of 12 dB, with a quantum channel typically shorter than 50 km, the secret key rate is 1.4 kbps.
- Entanglement-based QKD was also tested over a distance of ~1 km (~1dB loss), but the secure key rate obtained was rather low, being around 0.25 kbps as compared to a previous in-field test (in the SECOQC experiment, see later section) of 2 to 3 kbps.

[17] http://www.uqcc.org/QKDnetwork/

[18] "Field test of quantum key distribution in the Tokyo QKD Network", Opt. Express 19 (11), pp. 10387-10409, 2011, https://www.osapublishing.org/oe/fulltext.cfm?uri=oe-19-11-10387&id=213840

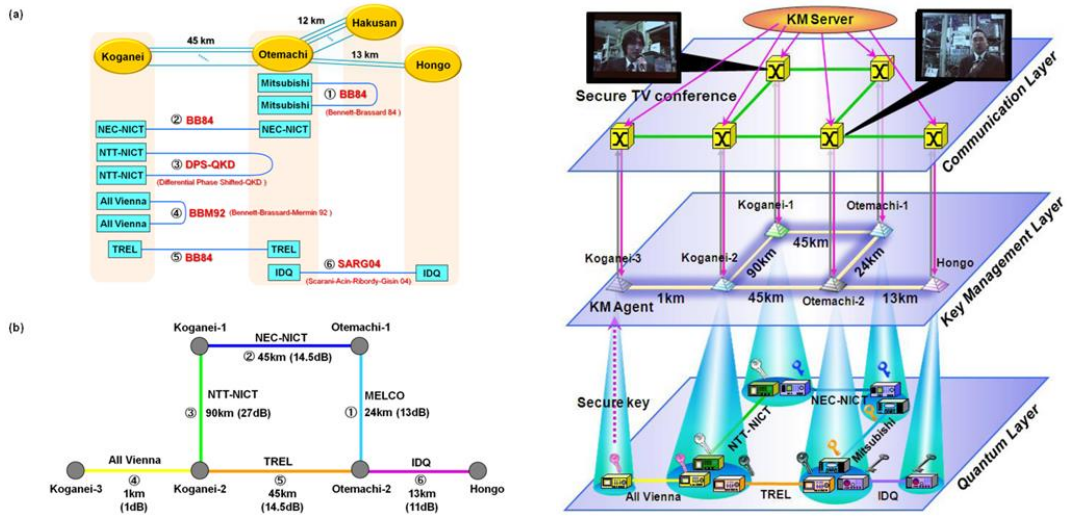


Fig. 5: topology and functional layers of the Tokyo quantum network. A live demonstration of secure TV conferencing, eavesdropping detection, and rerouting of QKD links was performed and made public in October 2010: a live video stream for was encrypted by OTP, with an encryption rate of 128 kbps. Secure keys were provided by over two routes, with total distances of 69 km and 135 km respectively.

In 2015 the Tokyo testbed was used by Toshiba to test a QKD "compact, robust and automatically stabilised" prototype[19]. On a 45km dark fibre, a total of 878 Gbit of secure key data over a 34 day period with diverse weather conditions is reported, corresponding to a sustained key rate of around 300kbps. The security analysis includes an efficient protocol, finite key size effects and decoy states, with a quantified key failure probability of $\varepsilon = 10^{-10}$, which equates to one key failure every 100,000 years.

In collaboration with Mitsubishi, Gakushuin University developed a CV-QKD system from off-the-shelf fibre components assembled in 19-inch rack mounts. The system was installed in the NICT facility and connected to the Tokyo QKD network. Tested on a 10 km quantum channel, the prototype generated a secure key rate of about 50 kbps[20]. More recently, CV-QKD has been demonstrated to generate a secure key rate (averaged over 24 hours) of 27.2 kbps with 100 classical channels (for a total of ~18 Tbps of traffic) co-propagating on a 10 km fibre, at 7 dB loss level[21].

The use of quantum effects beyond QKD to include protection of data at rest has also being demonstrated on the Tokyo testbed, by implementing an information theoretically secure distributed storage system via the combination of quantum key distribution with password-authenticated secret sharing [22]. It has however been pointed out that even with state-of-the-art secure key rates (~1 Mbps at ~50 km) this protocol cannot be employed in use cases of practical interest: securing realistic data size in a single data

[19] "High speed prototype quantum key distribution system and long term field trial", Optics Express Vol. 23, Issue 6, pp. 7583-7592, 2015
https://www.osapublishing.org/oe/abstract.cfm?uri=oe-23-6-7583

[20] "Implementation of continuous-variable quantum key distribution with discrete modulation", Quantum Sci. Technol. 2, 024010, 2017, https://iopscience.iop.org/article/10.1088/2058-9565/aa7230/meta

[21] "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3Tbit/s data channels", Communications Physics, Vol. 2, 9, 2019, https://www.nature.com/articles/s42005-018-0105-5

[22] "Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing", Scientific Reports volume 6, 28988, 2016, https://www.nature.com/articles/srep28988

centre would require much higher key generation rates, of the order of ~1Gbps [23]. An overview of the latest functionalities in the Tokyo quantum network has been presented at the ITU workshop on QKD in Shanghai in June 2019[24].

A proof-of-principle demonstration of QKD from a LEO orbit has been performed in 2016, using the SOTA (Small Optical TrAnsponder) laser communication terminal on board the LEO satellite SOCRATES (Space Optical Communications Research Advanced Technology Satellite). SOTA is a 6 kg terminal designed to carry out different laser communication experiments, and is equipped with a 5 cm telescope. Two non-orthogonally polarised signals in the ~800 m band modulated at 10 MHz were transmitted by SOTA and received in the single-photon regime by using a 1 m Cassegrain telescope. A QKD enabling QBER (Quantum Bit Error Rate) below 5% was measured with estimated key rates of the order of several kbps[25].

2.3 **South Korea**

Several field deployments are taking place. The government is funding the development of a ~ 250 km quantum backbone, see Fig. 6. South Korea Telecom started a Quantum Tech Lab in 2011, and in 2012 declared that it was aiming to build a deployable QKD system, advance the fabrication of QRNGs, and develop basic technologies for a quantum repeater[26]. The main use cases addressed are commercial metro network and 4G LTE commercial network, with a perspective on 5G.

[23] "Quantum networks: where should we be heading?", Quantum Science and Technology, Vol. 2, N. 2, 2017 https://iopscience.iop.org/article/10.1088/2058-9565/aa6994

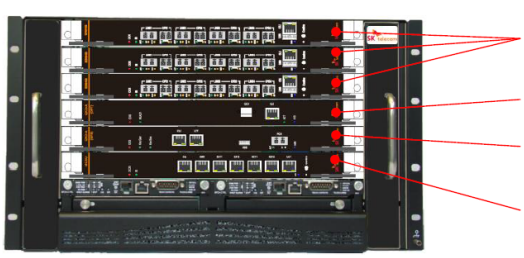
[24] "Tokyo QKD Network and its application to distributed storage network", ITU Workshop on Quantum Information Technology (QIT) for Networks, Shanghai, 2019, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Masahiro_Takeoka%20_V2_Presentation.pdf

[25] "QKD from a microsatellite: the SOTA experience", Proceedings Volume 10660, Quantum Information Science, Sensing, and Computation X, 106600B, 2018 https://arxiv.org/ftp/arxiv/papers/1810/1810.12405.pdf

[26] "Development of quantum communication technologies in SK telecom", 17th Opto-Electronics and Communications Conference (OECC 2012), July 2012, Busan, Korea. https://ieeexplore.ieee.org/document/6276393

Fig. 6: Deployment phases of the South Korean national QKD network[27].

A picture of the QKD system developed by SK telecom is shown in Fig. 7: it is based on the Advanced Telecommunication and Computing Architecture, specifies a secure key rate of 10 kbps over 50 km, and includes a 40 Gbps encryptor[28].



ATCA	
Chassis size	19 inch, 12U (14 slot) / 6U (6 slot); Shelf supplier dependent
QKD unit	2 slot
10Gbps encryptor unit	1 slot (bidirectional 4 ch.) ※ Max 80 slot (800Gbps)
Quantum key distribution	
Secure key rate	> 10 kbps @ 50km
Protocol	BB84 with unique phase modulation + decoy protocol and modified Winnow error correction
Random number generator	High speed quantum random number generator (2 Gbps)
Encryption	
Network protocols	10 GbE, STM64 (10 G SONET/OTN, 40G/100G Ethernet/OTN planned to be provided)
Algorithm	AES-GCM or ARIA-GCM
Latency	< 10 microseconds
Random number generator	Quantum random number generator

Fig. 7: the QKD system developed by SK Telecom[29]

In two of the locations where South Korea Telecom has by now deployed QKD systems it consistently obtained a secure key rate of 10 kbps over 50 km of dedicated quantum channel (see Fig. 8), and the QKD key has been employed to feed AES-256 encryptors: by multiplexing three 40 Gbps encryptor cards (each with 4 channels and 10 Gbps per channel) a total encryption speed of 120 Gbps has been achieved.

[27] https://www.photonics.com/Articles/Quantum_Networks_Photons_Hold_Key_to_Data/a60541

[28] "Status of QKD system deployment and ion trap development at SK telecom" http://www2.yukawa.kyoto-u.ac.jp/~rqin-2017/slides/Taehyun_Kim.pdf

[29] "Development of Quantum technologies at SK telecom", AAPPS Bulletin, Vol. 26 Issue 6, p2-9, 2016

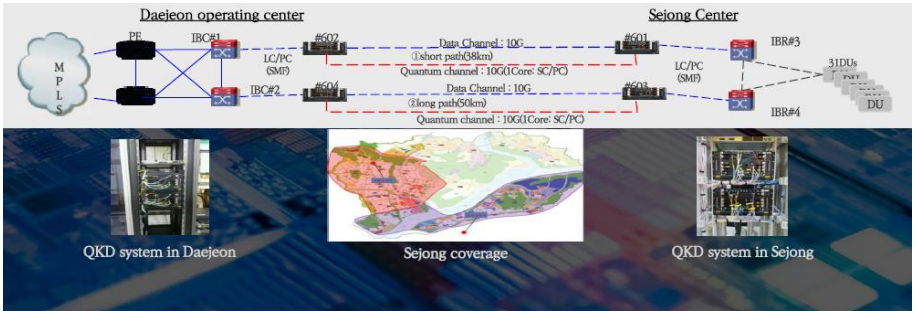


Fig. 8: QKD deployments by South Korea Telecom

In February 2018 South Korea Telecom bought, for ~$65 million, a controlling stake in the Switzerland-based firm ID Quantique[30], whose Clavis QKD system has been deployed within the SK Telecom LTE/5G network on the Seoul-Daejeon section and to the an LTE backhaul network between Sejong and Daejeon[31]. It recently announced collaboration with Nokia on QKD[32], revealed that it is applying its quantum security system to the trial network of Deutsche Telekom[33], and signed a ~$8.9 million deal supply contract with the U.S. quantum crypto communications company QuantumXchange[34].

SK Telecom is also active on standardisation, proposing new International Telecommunication Union (ITU) standards regarding quantum cryptographic systems and quantum random number generators (QRNG) with IDQ, Quantum Xchange, Florida Atlantic University and the University of Geneva.

3 Europe

3.1 Austria

The landmark project SECOQC "Development of a Global Network for SEcure COmmunication based on Quantum Cryptography" was a major research effort of 41 research and industrial organizations from the European Union, Switzerland and Russia, carried out between April 2004 and October 2008. It culminated in the deployment of a QKD network which was put into operation during the final SECOQC QKD conference held in Vienna from October 8 to 10, 2008[35]. The demonstration involved OTP-encrypted telephone communication, a secure (AES encryption protected) video-conference with all deployed nodes, and a number of rerouting experiments. The network consisted of eight point-to-point quantum links with an average length between 20 and 30 km (the longest one of 83 km), operated by QKD systems provided by:

[30] https://www.zdnet.com/article/sk-telecom-buys-half-of-swiss-quantum-safe-crypto-firm-for-65m/

[31] http://www.businesskorea.co.kr/news/articleView.html?idxno=23945

[32] https://www.prnewswire.com/news-releases/sk-telecom-and-nokia-sign-cooperation-agreement-for-quantum-cryptography-300413873.html

[33] https://pulsenews.co.kr/view.php?year=2018&no=473861

[34] http://www.businesskorea.co.kr/news/articleView.html?idxno=23945

[35] "The SECOQC quantum key distribution network in Vienna", New Journal of Physics, Volume 11, July 2009 https://iopscience.iop.org/article/10.1088/1367-2630/11/7/075001/meta

- ID Quantique: three plug and play systems (based on the commercial Cerberis system)
- Toshiba Research Europe: one way weak pulse system
- GAP Optique, with ID Quantique and AIT Austrian Institute of Technology: coherent one-way system
- University of Vienna and AIT: entangled photon system
- CNRS, with Thales and Université Libre de Bruxelles: continuous-variable system
- Munich Ludwig Maximillians University: a free space 80 m link

The network topology and a photograph of the QKD systems implemented at the nodes are shown in Fig. 9. All the QKD hardware had to comply with interoperability and performance criteria, providing a key generation rate in excess of 1 kbps at a 6 dB loss level (equivalent to a distance of ~25 km over standard telecom fibre with ~0.25 dB/km attenuation). Fig. 10 shows the performance of two of the deployed systems.

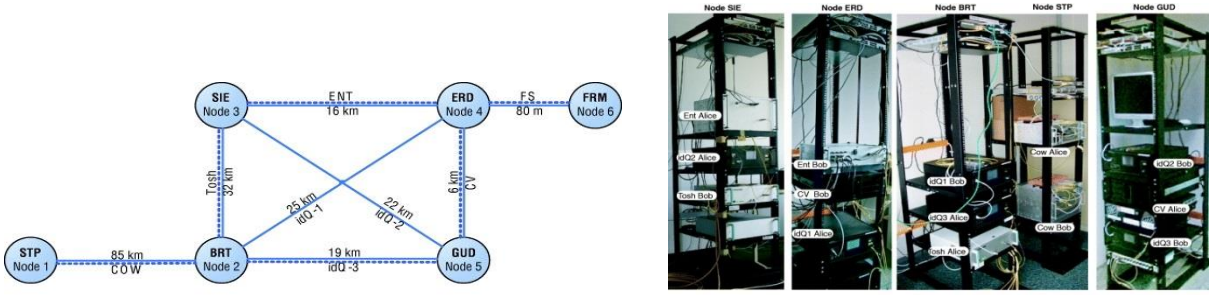


Fig. 9: SECOQC network topology and quantum hardware implementation

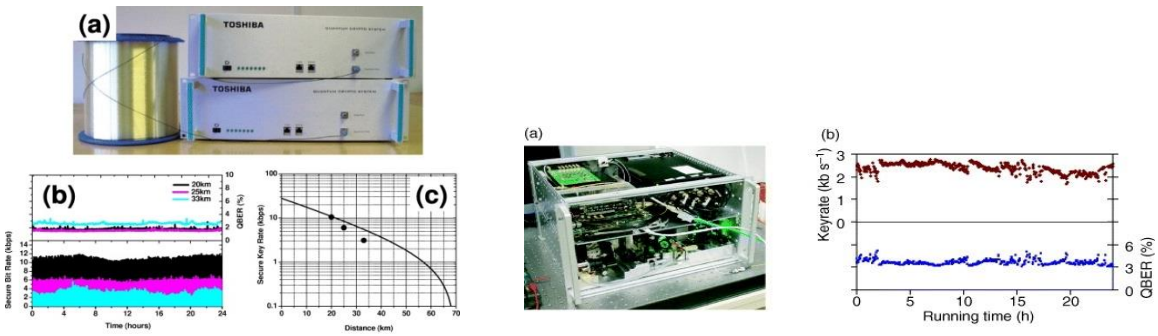


Fig. 10: Performance of the Toshiba system and of the entanglement-based one.

The overall architecture of the testbed is shown in Fig. 11. A number of standard communication utilities such as IP telephony and IP-based video-conferencing have been tested, with end-to-end security guaranteed by a virtual private network (VPN) tunnel. A one-time pad tunnel is realized between two application servers running on PCs, directly connected to corresponding node modules. Pay-load data can be sent directly over the OTP tunnel, in which case ITS transmission security is theoretically obtained, or by using a standard IPsec tunnel based on AES encryption and authentication, with frequent key exchange. The AES-key is typically changed every 20 s, and the consumed key rate does not depend on the actual size of the plaintext message that is to be encrypted.

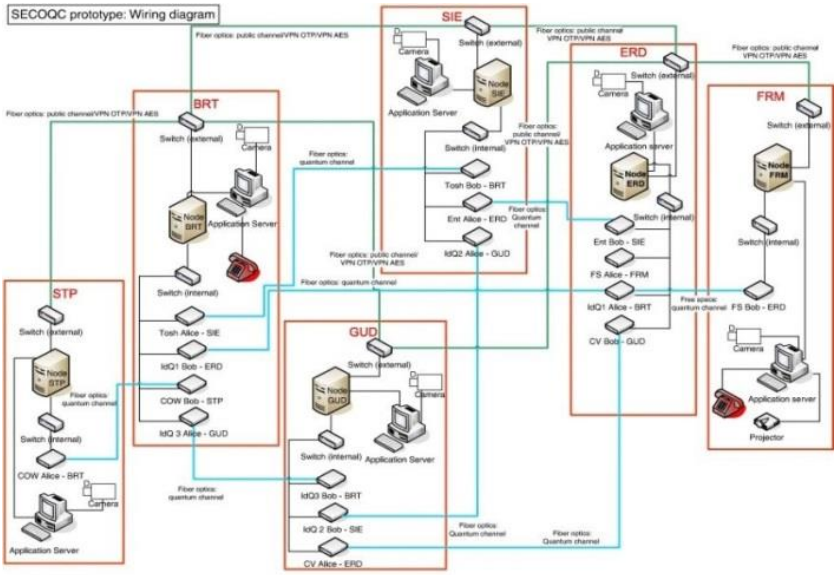


Fig. 11: application layout of the SECOCQ testbed

3.2 **Switzerland**

The quantum network deployed by the SwissQuantum project focused on network features linked to performance, flexibility and reliability, and was the first one to operate continuously on a long term, from March 2009 to January 2011[36]. It operates on three functional layers, as detailed in Fig. 12: (i) a quantum layer composed of QKD point-to-point links implemented with the commercial ID Quantique 5100 device (ii) a key management layer in charge of the management of secret keys, and (iii) an application layer where the keys are used by the end-user applications

[36] "Long term performance of the SwissQuantum quantum key distribution network in a field environment" https://arxiv.org/ftp/arxiv/papers/1203/1203.4940.pdf

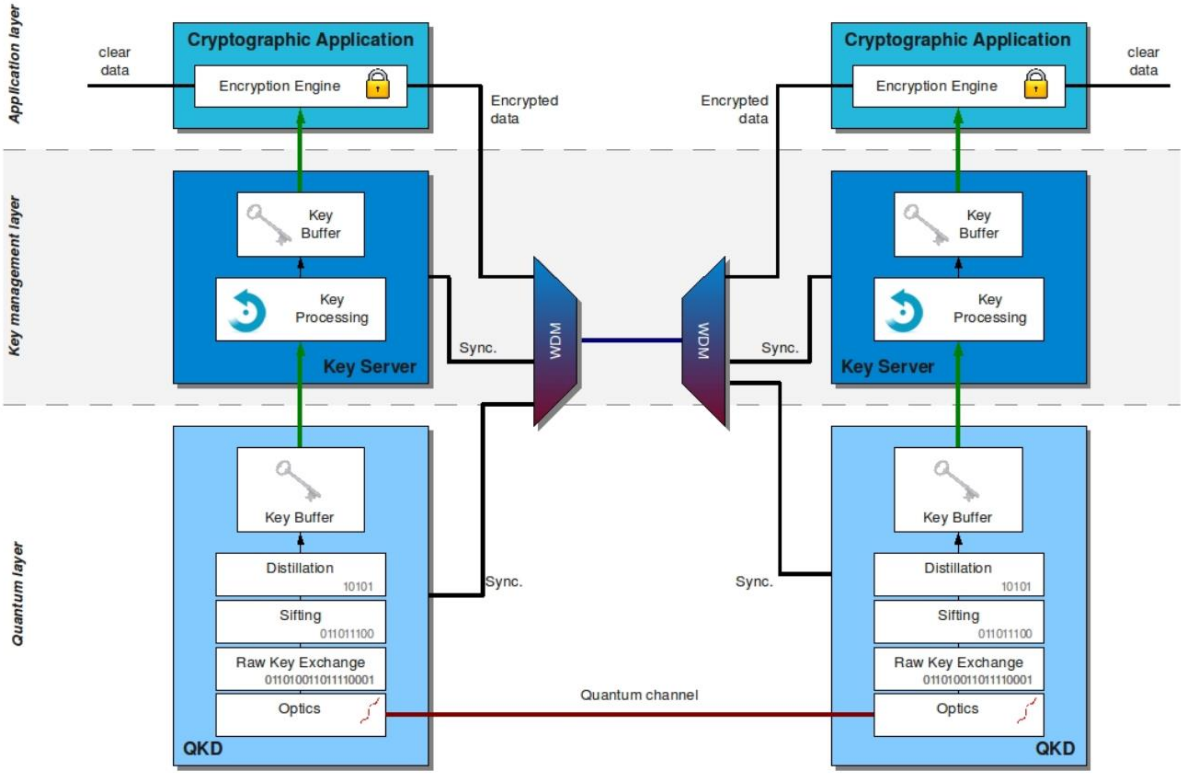


Fig. 12: The functional layers of the SwissQuantum network.

Different commercial encryptors (10 Gbps Ethernet, 2 Gbps Fibre Channel, and IPsec) made use of the quantum keys distributed by ID Quantique equipment, taking advantage of a dual-key agreement protocol, where the final encryption key is the cyphertext of a key obtained from a Public Key Infrastructure, OTP-encrypted with the key obtained by QKD: the keys exchanged with quantum cryptography and the keys exchanged via the PKI are combined to obtain the final key, which will be as secure as the more secure among the two initial keys. The work was not aimed explicitly at implementation security, and did not consider threats such as quantum hacking. It consisted of 3 nodes linked by a 3.7 km (2.5 dB loss), a 14.4 km (4.6 dB loss), and a 17.1 km (5.3 dB loss) dark fibre for the quantum channel, see Fig. 13. The average number of 256-bit AES keys distributed per each day of operation was ~300 000 for the higher loss links and ~800 000 for the lower loss link. This last figure corresponds to a secure key rate of 800 000×256/(24×60×60) = 2.4 kbps.

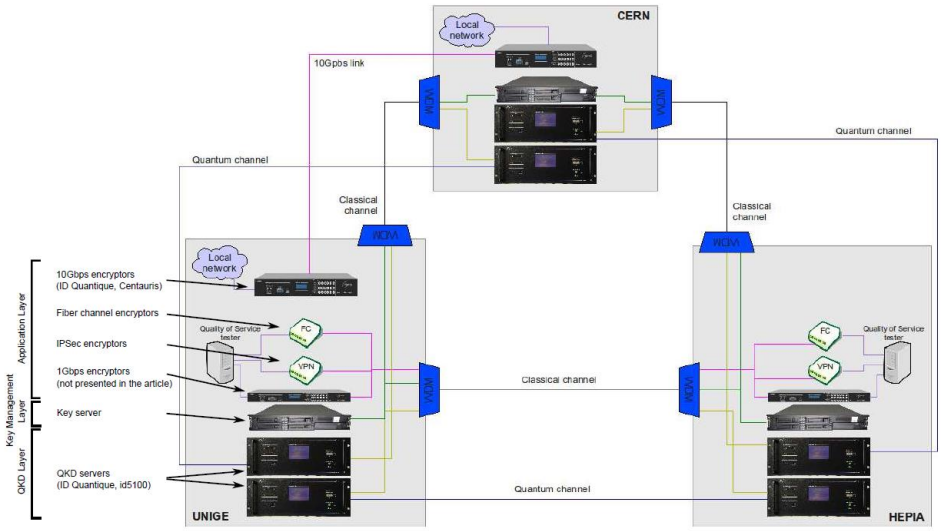


Fig. 13: architectural implementation of the SwissQuantum network.

3.3 **Italy**

The "Italian Quantum Backbone" (IQB) has been developed during the period 2013 to 2019 by the Istituto Nazionale di Ricerca Metrologica (INRiM), in collaboration with the Consiglio Nazionale delle Ricerche (CNR). Originating from fibre-optic infrastructure used for the dissemination of precise time and frequency signals generated by atomic clocks, it is being upgraded to include quantum channels suitable for QKD. IQB now comprises ~1 860 km of fibre connecting several cities; it was funded with ~6 million euro over 5 years, and the fibres were secured for 15 years. It is mainly composed of a pair of dark fibres, with the exception of ~300 km which are in data-traffic sharing. One fibre is typically reserved for the quantum channel, while the other hosts the time over fibre service, typically using the "White Rabbit" protocol, and dense wavelength division multiplexed (DWDM) classical data traffic. Researchers have full access 24 hours a day, 7 days a week, and equipment can be hosted in cabins along the fibre (every 50-100 km), in dedicated buildings with restricted access. Metropolitan area networks are possible in the connected cities, in particular in Turin, Milan, Florence, Rome, Naples. Extensions towards France, Switzerland, Austria, and Germany are being deployed, with the final aim of a pan European network for time and frequency distribution, see Fig. 14.

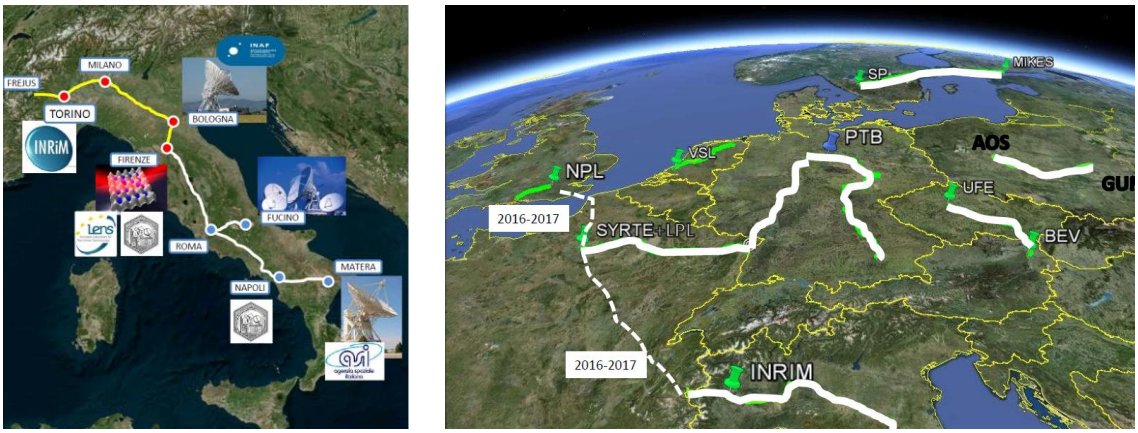


Fig. 14: the Italian quantum backbone and the European time and frequency distribution network

The backbone is presently being used by several research institutes (e.g. CNR in Florence and Naples, INAF in Bologna, ASI in Matera) for radio astronomy, atomic and molecular physics, relativistic geodesy, and other scientific applications. It has a customer of time-stamping services for high frequency financial trading, and several industrial players have also expressed their interest for services such as smart grid and 5G network synchronisation, time distribution to the GNSS ground segment, calibration, etc.

A QKD experiment have been performed on the 100 km Torino-Santhià link, where a ~30 dB loss has been measured: an ID Quantique Clavis3 system was employed with two Stirling motor cooled ID Quantique ID230 single photon detectors, and a key rate of 0.25 kbps was obtained.

A second field demonstration of a complete QKD system was performed over a dark fibre link situated in Florence, with a total loop-back length of 40 km and 21 dB of transmission losses, see Fig. 15. A three-state BB84 protocol with time-bin encoding was demonstrated to enable a secret key rate of ~3.4 kbps (including a finite-key analysis), with the synchronisation signal propagating alongside the quantum one in the C-band. Work is ongoing to deploy a second quantum link, over a 21 km fibre: in this case a single ITU channel will be used to transmit the quantum signal, with 10 Gbps of data traffic running in parallel. It is also planned to test CV-QKD.

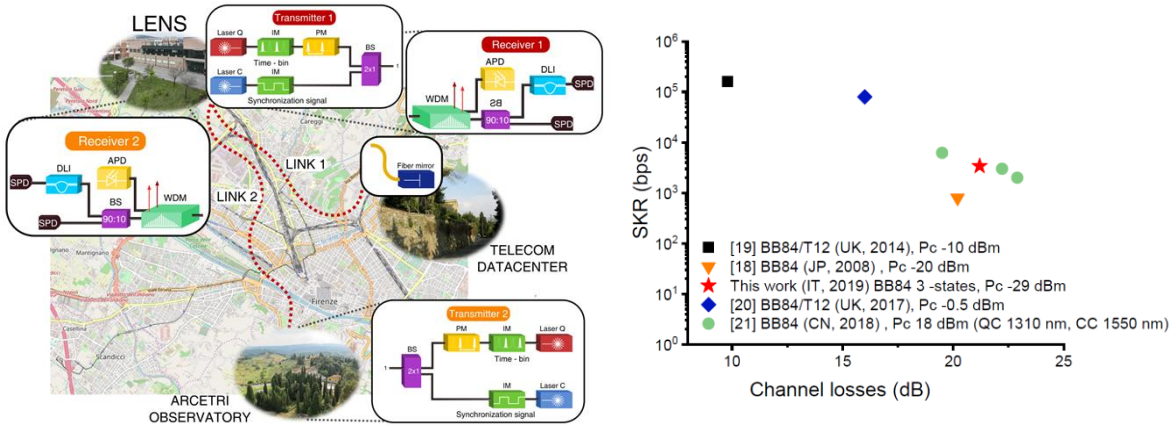


Fig. 15: discrete variable QKD system over 40 km of loop-back dark fibre link (Link 1), and performance comparison with other field experiments[37]. Coexistence with DWDM traffic will be tested on the 21km LINK 2.

A QKD link between Sicily and Malta, over ~100 km of dark fibre in an undersea cable with ~30 dB loss is planned; it is proposed to use a single photon quantum signal at 1 550 nm, up-converted to 863 nm for detection by high-efficiency, low-dark-count silicon diodes.

The Sicily to Malta fibre link has also been used to demonstrate in-field entanglement distribution: the quality of entanglement shows that the quantum prerequisites are satisfied which would allow implementing QKD with key rates of 57.5 bits per second[38].

[37] "Field trial of a finite-key quantum key distribution system in the Florence metropolitan area", https://arxiv.org/pdf/1903.12501.pdf

[38] "Entanglement distribution over a 96-km-long submarine optical fiber", PNAS 116 (14) 6684-6688, 2019 https://www.pnas.org/content/116/14/6684

Several experiments[39,40,41] demonstrating quantum links with satellites have been performed using the 1.5 m telescope hosted by the Matera Laser Ranging Observatory (MLRO, which is connected to the backbone, see Fig. 16), and work to establish a quantum link between MLRO and the Chinese quantum satellite is ongoing.

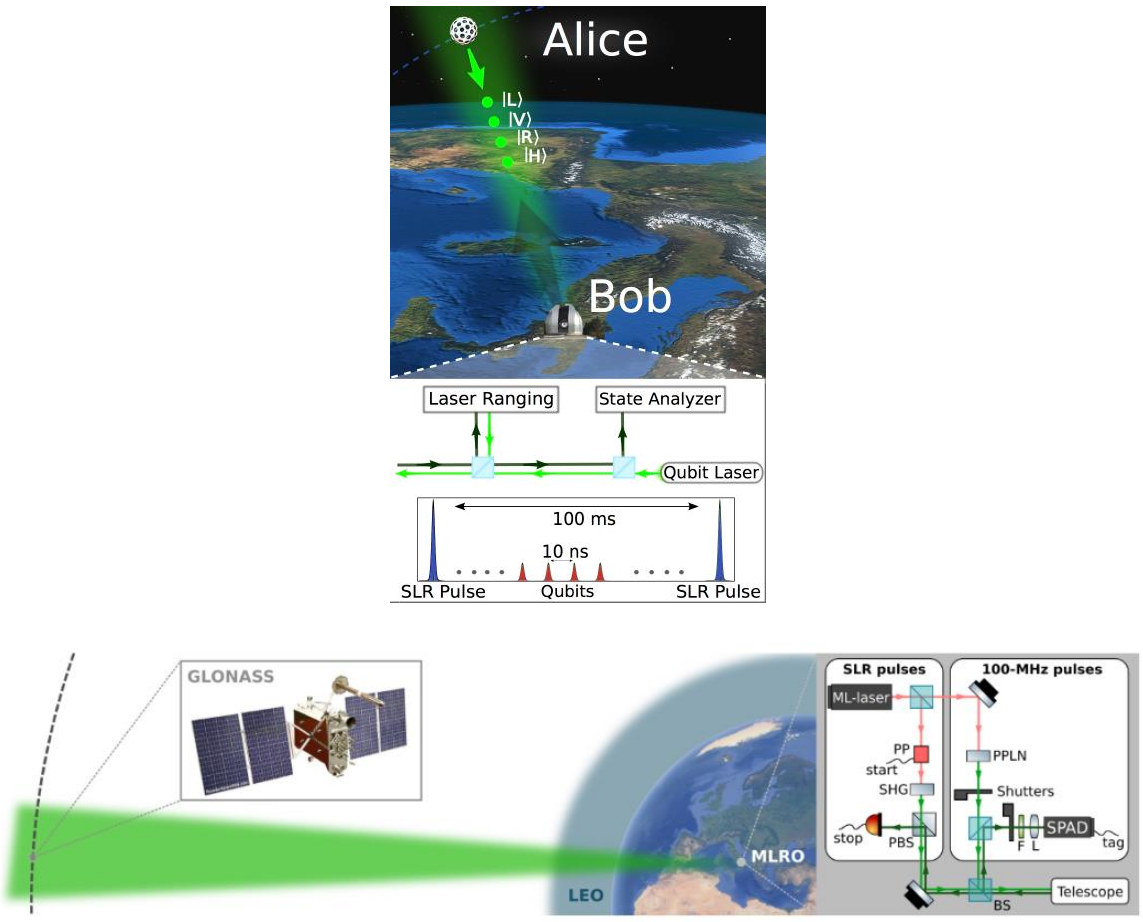


Fig. 16: space quantum communications with LEO satellites and with a GNSS (MEO) satellite.

3.4 **Spain**

Work on QKD real-field deployments in Madrid started in 2009, and is now being carried on in collaboration between Universidad Politécnica de Madrid, Telefónica de España, and Huawei[42]. In the Spanish quantum network, the links are of modest distance; work has instead concentrated on integration of QKD into operational telecommunications and data networks, especially in the software layers. The first network[43] studied the feasibility of

[39] "Experimental Satellite Quantum Communications", Phys. Rev. Lett. 115, 040502, 2015 https://arxiv.org/pdf/1406.4051.pdf

[40] "Towards quantum communication from global navigation satellite system", Quantum Science and Technology, 4 (1): 015012, 2018, https://arxiv.org/pdf/1804.05022.pdf

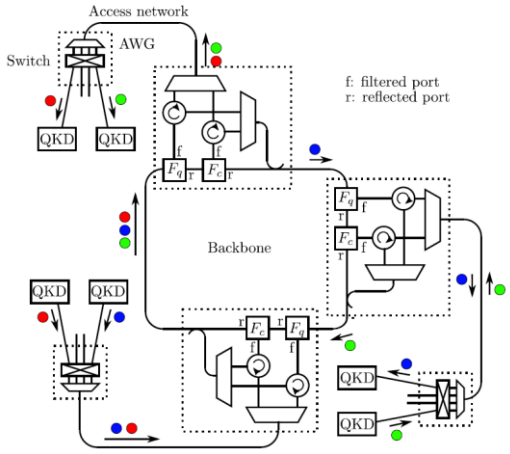
[41] https://quantumfuture.dei.unipd.it/

[42] http://www.gcc.fi.upm.es/

[43] "QKD in Standard Optical Telecommunications Networks ", International Conference on Quantum Communication and Quantum Networking, 2009 http://www.gcc.fi.upm.es/publications/978-3-642-11731-2_18.pdf

serving a metropolitan area network, including a backbone and an access gigabit passive optical network (GPON) at 2.4 Gbps, without resorting to trusted repeaters. Two commercial ID Quantique QKD systems were used, with the quantum channel at 1 550 nm and concurrent classical traffic at 1 510 and 1 470 nm. In the backbone a secure key rate of ~500 bps was obtained for distances up to 6 km, while in the GPON the secure key rate is ~500 bps at 0 km, reduced to 20 bps at 3.5 km. These numbers suggests that quantum and classical signals can be mixed to provide acceptable performances in a metro-scale infrastructure, serving up to 4 simultaneous users in the GPON with a fast renewal of 256-bit AES keys.

The second generation network[44] was used to investigate how many simultaneous users a quantum network could support using standard telecommunications equipment, an issue which is of paramount importance for the definition of a commercial use case. End-to-end quantum links, without trusted repeaters and each one below a maximum loss budget of 30 dB were implemented on the network shown in Fig. 17.



Device	Passband	Losses
Single-mode fiber	C band	0.18 dB/km
Single-mode fiber	O band	0.32 dB/km
Connectors	—	0.2 dB/pair
1×2 Splitter	$1270-1350\&1510-1590$ nm	3.6 dB
1×32 Splitter	$1270-1350\&1510-1590$ nm	16.5 dB
4×4 to 192×192 Switch	—	1 dB
Circulator	$1280-1340$ nm	0.8 dB
Circulator	$1520-1580$ nm	0.8 dB
CWDM filter	≈ 13 nm	$0.4-0.6$ dB
1310/1550 WDM mux	$1260-1360\&1460-1560$ nm	0.5 dB
32-ch AWG DWDM mux	100 GHz	3 dB

Fig. 17: QKD Metropolitan Area Network with three access networks, and table with the typical optical loss introduced by its components.

The quantum and the corresponding classical channel (in the ~1 300 nm and ~1 500 nm bands respectively) of a given QKD device were automatically and passively directed by the network to the same destination, which can be located in any of the access networks connected to the core. It was demonstrated that up to 32 simultaneous QKD links can simultaneously be supported with a QBER below 6%, which allows for the distillation of a secure key, each one with a concurrent classical traffic of up to 1.25 Gbps.

Apart from securing users traffic, QKD can be employed to add an additional security layer to the communication infrastructure itself. This is especially important given the current trends toward software-defined networking (SDN) and network function virtualisation (NFV) paradigms, which allow more dynamic and flexible infrastructures and architectures. From one side, SDN and NFV enable operators to automate the setup of services, thus reducing costs in deploying and operating the required infrastructure. On the other hand, they expose the infrastructure to new vulnerabilities, as critical

[44] "Quantum metropolitan optical network based on wavelength division multiplexing", Optics Express, Vol. 22, No. 2, 2014, https://www.osapublishing.org/oe/abstract.cfm?uri=oe-22-2-1576

information travels from central offices to remote data centres and network devices[45]. A telecommunication network includes points of presence that are considered secure places, which are usually separated by distances of the order of 50 km. Such a structure can therefore support QKD in the trusted nodes approach, and use the quantum keys to secure the control plane.

The three-node Madrid Quantum Network (see Fig. 18) will be employed to explore the possibility of including QKD devices in SDN, seamlessly integrating quantum security in commercial telecom networks without the need of ad-hoc modifications. The QKD systems which are being developed by Huawei are based on continuous variable protocols. The same fibre will be employed in the same optical band by the quantum channel and more than 20 classical data channels, allowing ~2 Tbps of data using the standard 100 Gbps communications technology usually employed in metropolitan area networks.

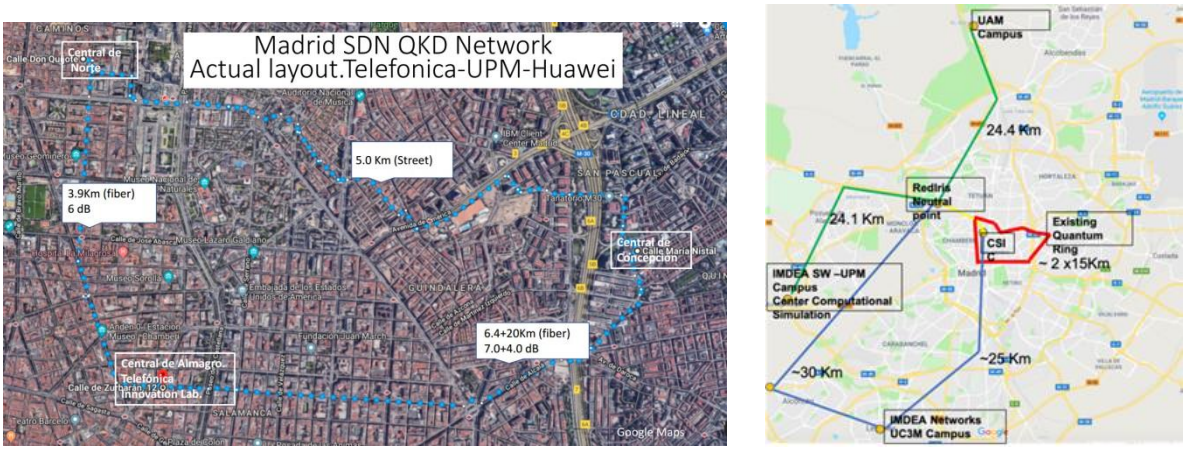


Fig. 18: Core of the Madrid Quantum Network installed in Telefónica Production Facilities, and extended Madrid Quantum Network. The red ring connects the core production facilities, and the yellow link will join the production network with the RedIMadrid network (courtesy Universidad Politécnica de Madrid).

3.5 **UK**

Construction of the UK quantum network (UKQN), a fibre-based network across the south of England, is the principal project of the quantum communications hub of the UK national programme in quantum technologies[46]. The metropolitan networks in Cambridge and Bristol will be linked via London and Reading over the National Dark Fibre Infrastructure Service (NDFIS), with extensions to the University of Southampton and the National Physical Laboratory (NPL) in Teddington (Fig. 19). The technology is supplied by ID Quantique, Toshiba, ADVA, and BT; Toshiba is, in particular, testing, on some links of the network, its QKD prototype, which is based on a single-photon protocol using phase encoding[47]. NPL is working with all the partners to develop the measurements necessary to help assess the security of the network's distributed QKD keys. NPL already provides precise time to the City of London financial centre.

[45] "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks", IEEE/OSA Journal of Optical Communications and Networking, Vol. 9, Issue 10 , 2017
http://www.personal.fi.upm.es/~jmartinez/publications/JOCN.9.000819.pdf

[46] https://www.quantumcommshub.net/

[47] Technical specifications available on the Toshiba website https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/

Fig. 19: segments of the UK Dark Fibre Network under testing for QKD deployments.

On the Cambridge-Duxford segment a three-week test has been made in a looped-back fibre with a total length of 66 km and 16 dB link loss; 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. The mean secure key rate observed was 80 kbps, with a standard deviation of 28 kbps[48]. The section between Cambridge and Telehouse in London is a single span of 120 km without trusted nodes, with ~29 dB loss and a secure key rate of ~2 kbps[49]. In the section linking the Cambridge Science Park (location of Toshiba Research Europe Ltd. - TREL) to Adastral Park (BT's research campus near Ipswich) a standard BT fibre carries both quantum and non-quantum traffic, and 500 Gbps of encrypted data secured by quantum keys are transmitted across 120 km multiple hop deployed fibre network, with BT exchanges acting as trusted nodes (see Fig. 20)[50].

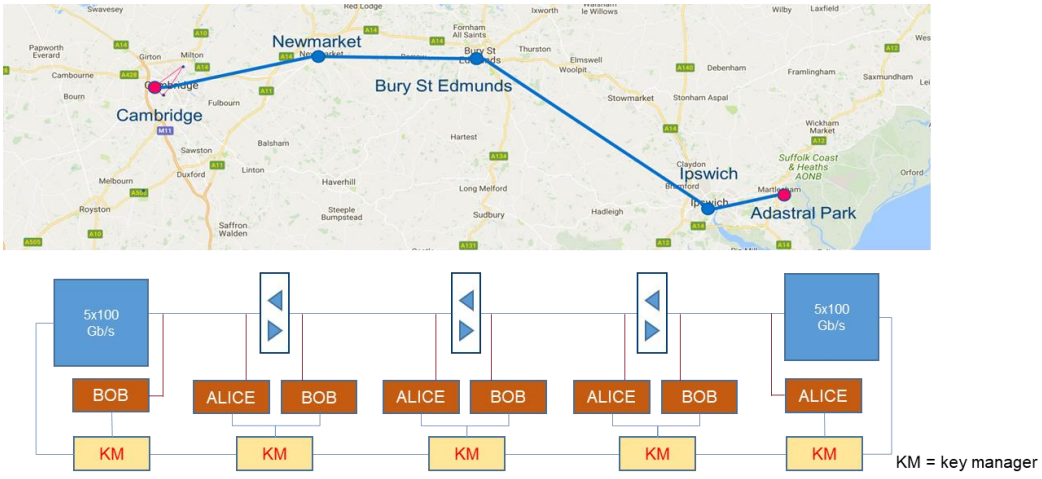


Fig. 20: quantum link deployed between Cambridge and BT labs, with trusted nodes.

[48] "Field trial of a QKD and High Speed Classical Data Hybrid Metropolitan Network", Proc. SPIE 10559, Broadband Access Communication Technologies XII, 1055907, 2018, http://spie.org/Publications/Proceedings/Paper/10.1117/12.2290544

[49] Private communication, to be published

[50] "Field trial of a QKD and high-speed classical data hybrid metropolitan network", Photonics West 2018, paper 10559-6, San Francisco, 2018

Metropolitan networks are also in operation within Cambridge and Bristol. QKD systems developed by TREL have been tested for several months in the Cambridge quantum network, on fibre spans with lengths of 5.0 km, 9.65 km and 10.4 km (having respectively losses of 1.2 dB, 3.3 dB and 3.4 dB), see Fig. 21. The average secure key rates observed during the testing period on the three links were 3.2 Mbps, 3.2 Mps, and 2.5 Mbps respectively on dark fibres, while in the presence of concurrent 200 Gbps classical data the secure key rates reduce respectively to 2.9 Mbps, 2.7 Mbps, and 1.4 Mbps[51].

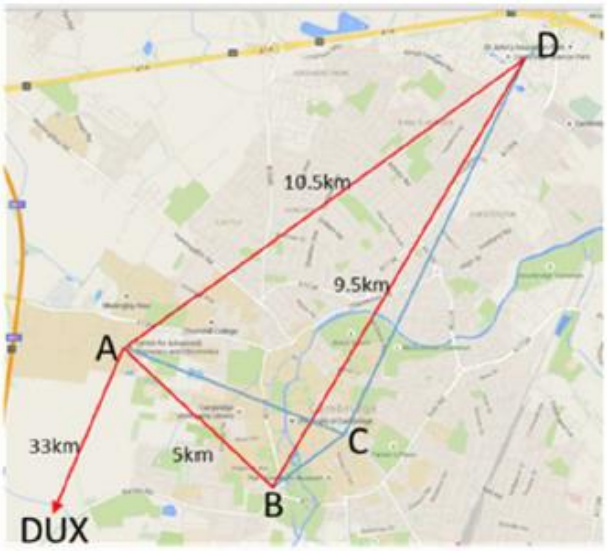


Fig. 21: The Cambridge Fibre network. A: Electrical Engineering building; B: Engineering Department; C: University central network facility; D: Toshiba Research Europe Cambridge Laboratory; DUX: dark fibre link to Duxford.

The Bristol metropolitan area quantum network was formally opened in September 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[52].

3.6 **Russia**

According to recent information, the 5-years "Data Economy" programme (2019-2024) adopted by the Russian government includes $0.7 billion government funding for Quantum Technologies. In the last ~5 years several QKD testbeds have been set up, and QKD is now seen as an "industry-ready" technology, see Fig. 22 and Fig. 23[53].

[51] "High performance field trials of QKD over a metropolitan network", QCrypt 2017 - 7th International Conference on Quantum Cryptography, Cambridge, UK, 2017
http://2017.qcrypt.net/wp-content/uploads/2017/09/Th467.pdf

[52] https://www.bristol.ac.uk/physics/research/quantum/conferences/qkdover5guk/

[53] Quantum communication in Russia: status and perspective, ITU Workshop on Quantum Information Technology for Networks, Shanghai, China, June 2019, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Vladimir%20_Egorov_Presentation.pdf

The Information Technologies, Mechanics and Optics (ITMO) state university has deployed a quantum link in St. Petersburg using the modulated sideband protocol[54]. The qubits at 1 550 nm were transmitted along a 1 km dedicated underground fibre, with an overall loss of 1.63 dB. Russian-made superconducting nanowire single photon detectors have been used to obtain a sifted key rate of ~1 Mbps at a ~1% QBER level; no privacy amplification was carried out, and thus no secure key was obtained. The same technology is planned to be used to establish a quantum link in Kazan along a distance of 160 km, with an overall loss of 45 dB. A group of ITMO researchers founded a QKD start-up named Quantum Communications LLC, which in 2016 secured a 340 000 euro contract.

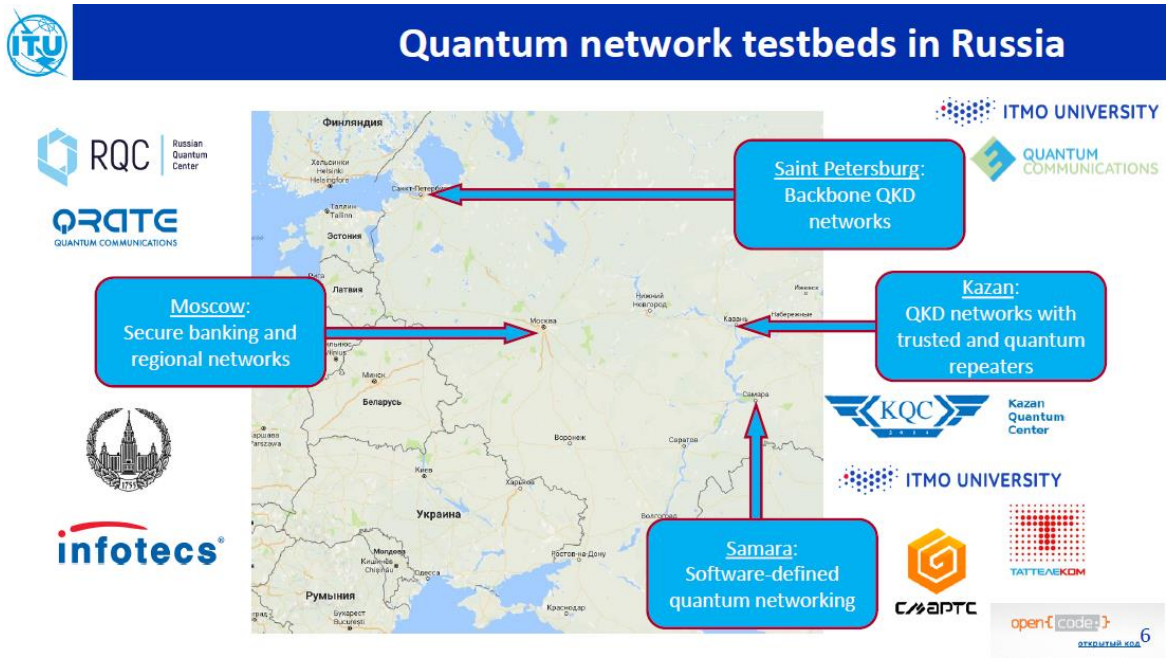


Fig. 22: QKD testbeds in Russia

[54] "Sideband quantum communication at 1 Mbit/s on a metropolitan area network", Journal of Optical Technology, Vol. 84, No. 6, 2017, https://www.osapublishing.org/jot/abstract.cfm?uri=jot-84-6-362

Fig. 23: Main Russian players in QKD

In Moscow, the Russian Quantum Center has started serial production of QKD systems, having performed several live demonstration of QKD-secured links[55], launched a quantum network connecting Gazprombank offices[56], and a quantum link between Sberbank offices. A decoy state polarization-encoded QKD protocol is employed at 1 550 nm along two links of 30 km (13 dB loss) and 15 km (7 dB loss), establishing a secure key rate of 0.1 kbps and 0.2 kbps respectively, with an operational security parameter smaller than 5×10^{-11}; ID Quantique ID230 single photon detectors have been employed[57]. In a further deployment, a link of 25 km was tested with a total loss of 20 dB: the QBER was in the 4.8%-6% range, and a secure key rate of 0.1 kbps was established, with a similar operational security level[58]. The secure key has been used for continuous key renegotiation in a VPN tunnel according to the Russian standardised 256 bit algorithm GOST 28146-89. The key is refreshed every 40 s, and sustains a data transfer rate of 1 Gbps.

Future plans contemplate a ~15 000 km transcontinental QKD line, to unify Chinese and European infrastructure, and the development of a satellite QKD system with a 1-10 kbps secure key rate used to secure a ~10 Gbps optical channel. The ground station is under preparation, and work for the QKD payload will start in 2010; the satellite launch is envisaged for 2023, to be followed by the development of an orbital group.

[55] http://news.ifmo.ru/en/news/8551/

[56] https://www.gazprombank.ru/en/press/4807247/

[57] "Quantum-secured data transmission in urban fibre-optic communication lines", Journal of Russian Laser Research, Volume 39, Issue 2, pp 113–119, 2018, https://arxiv.org/pdf/1712.09831.pdf

[58] "Demonstration of a quantum key distribution network in urban fibre-optic communication lines", Quantum Electronics, Volume 47, Number 9, 798–802, 2017, https://arxiv.org/abs/1705.07154

3.7 **Poland**

Work for a three-node QKD link in Wroclaw (see Fig. 24) was announced in 2014, but no information about actual implementation has been made available in the last five years[59]. Extensive experience in laboratory testing of commercial and pre-commercial QKD equipment has however been acquired, including feasibility tests for QKD deployment in real-world optical fibres networks[60].

Fig. 24: planned QKD deployments in Wrocław

4 North America

4.1 **USA**

The first fibre-based QKD network worldwide was funded by DARPA: it started operating in June 2004, securing a fibre-optic loop connecting facilities at Harvard University, Boston University, and the office of BBN Technologies in Cambridge (Massachusetts) for a total of six nodes (see Fig. 25)[61]. Different hardware platform were developed by BBN, BU, NIST and QinetiQ, and tested in the field.

- BBN: Phase-modulated weak-pulses at 1 550 nm
- BBN & BU: polarization-entangled photons at 1 550 nm via fibre;
- NIST: free space at ~850 nm
- QinetiQ: free space.

Actual delivery of secret key was demonstrated to be possible by phase-modulated weak pulses along the BBN-Harvard span (10.2 km length, 5.1 dB loss), with 1000 bps of privacy-amplified secret key. It was not possible to establish a secure key along the BBN-BU span (19.6 km length with 11.5 dB loss). The performance of the DARPA network is reported here for its historical interest, and because it can be taken as the starting point of QKD field deployments. The network apparently stopped operating in 2006 and no other field deployments by USA government agencies since then are known.

[59] https://seqre.net/seqre2014/wroclaw.php

[60] "Quantum key distribution security constraints caused by controlled quality of dark channel for non-entangled and entangled photon quantum cryptography setups", Optical and Quantum Electronics, Vol. 48, No. 363, 2016, https://link.springer.com/article/10.1007/s11082-016-0624-9

[61] "Current status of the DARPA Quantum Network", presented at the Defense and Security Conference, Orlando, Florida, 2005. Proceedings published in Quantum Information and Computation III, Volume 5815, (2005), https://arxiv.org/ftp/quant-ph/papers/0503/0503058.pdf

Los Alamos National Laboratories are working with Oak Ridge National Laboratories and a utility company to advance the use of QKD to secure the energy grid[62].

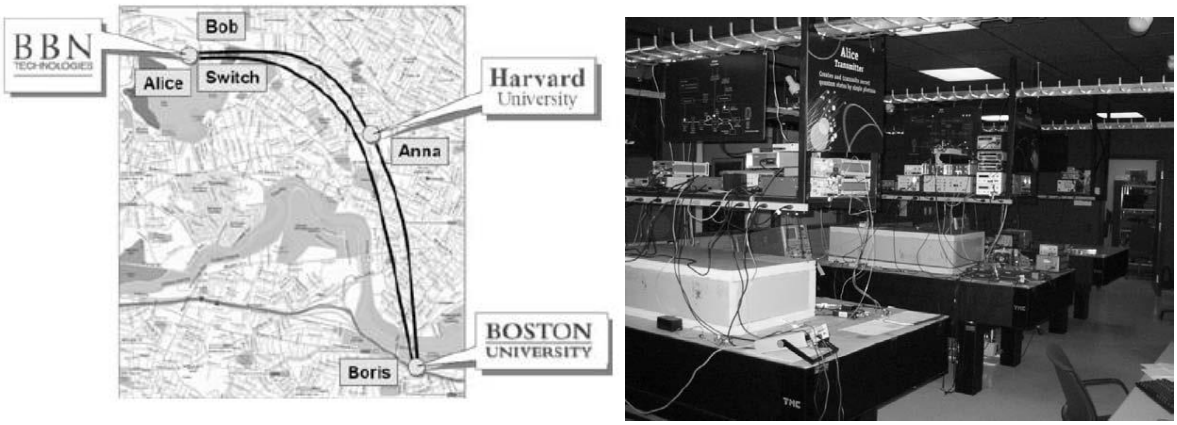


Fig. 25: the DARPA quantum network in Cambridge, Massachusetts

Batelle, a private non-profit company, was the first to deploy a QKD network for internal use, starting from 2013 and using ID Quantique hardware[63]. As shown in Fig. 26, Batelle linked their headquarters in Columbus to a production facility in Dublin (Ohio) with a dedicated unlit fibre: using Cerberis QKD equipment combined with a Centauris encryptor provided a 1 Gbps link with Layer 2 encryption. Ambitious plans to reach their offices in Washington (DC), via trusted nodes with a ~700 km backbone have apparently been shelved.

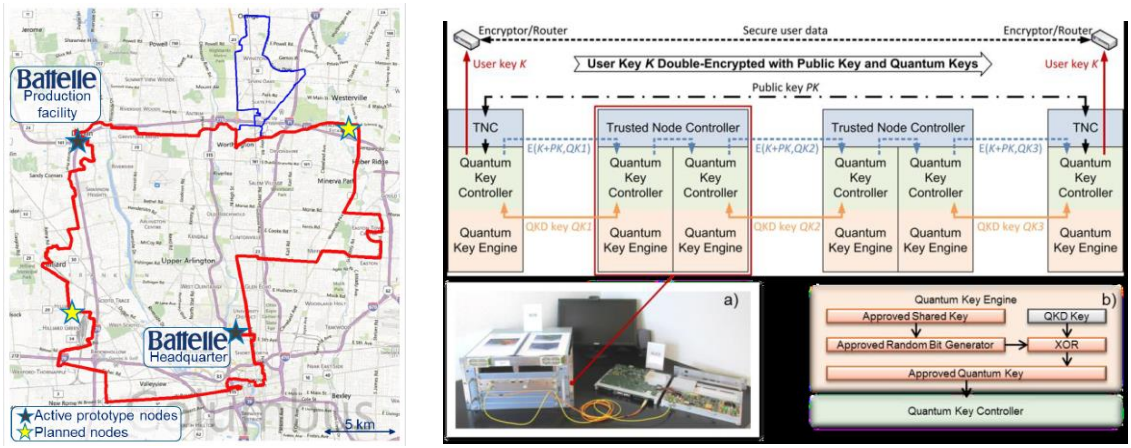


Fig. 26: Batelle QKD network in central Ohio, with a 25 km long loop[64], and its architectural implementation. The apparatus provides a QKD secret key rate of ~1 kbps over fibre links with less than -19 dB transmission.

In February 2018 a company named "Quantum Xchange" unveiled plans to link Boston with Washington via an 800 km trusted-nodes link based on dark fibres, supplied by the

[62] "Los Alamos teams with Oak Ridge, EPB to demonstrate next-generation grid security tech", Los Alamos National Laboratory website, February 2019
https://www.lanl.gov/discover/news-release-archive/2019/February/0212-grid-security-tech.php

[63] https://www.battelle.org/case-studies/case-study-detail/quantum-key-distribution

[64] "Towards a North American QKD Backbone with Certifiable Security", Nino Walenta et al, QCrypt 2015
http://2016.qcrypt.net/wp-content/uploads/2015/09/Contributed1_Nino-Walenta.pdf

communications infrastructure provider Zayo[65]. A $10 million funding round has already been completed. Quantum Xchange said it will start by connecting Wall Street's financial markets with back-office operations based in New Jersey offering, on a subscription basis, a QKD service designed for banks and other financial institutions that need to ensure their data is safe and secure[66]. Quantum Xchange is currently exploring the availability of QKD hardware: technical collaboration with Toshiba seems to be ongoing[67], and a communication system supply contract worth 10 billion won was signed with South Korea Telecom via ID Quantique[68,69]. No talks with potential developers from the USA have been reported: indeed the activity on QKD technological development by USA commercial players seems to have peaked in 2008[70].

The Office of Advanced Scientific Computing Research of the Department of Energy has published in 2018 a document advocating the deployment of a "Quantum Network for Open Science", which will provide QKD alongside sensing and computation, see Fig. 27. Its deployment could take advantage of the DOE High-Performance Optical Backbone Network. Chicago (with Argonne national laboratories, FermiLab, University of Chicago, and University of Chicago at Urbana Champaign) is likely to become a DOE hub in quantum networking, with an authorized funding level up to $60 million for 5 years. There is an ongoing debate on forming a National Science Foundation quantum networking hub between MIT/Harvard, Stanford and Caltech, with a possible funding of $25 million for 5 years. The emphasis seems however to be on quantum communication as a way to leverage distributed quantum computing, rather than on QKD.

[65] https://quantumxc.com/

[66] https://siliconangle.com/2018/06/26/quantum-xchange-build-first-quantum-network-u-s-offering-unbreakable-encryption/

[67] https://optics.org/news/10/4/50

[68] https://www.idquantique.com/quantum-xchange-and-id-quantique-make-ultra-secure-quantum-networks-a-reality-for-leading-us-industries/

[69] http://www.businesskorea.co.kr/news/articleView.html?idxno=23945

[70] "The impact of quantum technologies on the EU's future policies. Quantum communications: from science to policies", JRC report, 2018
http://publications.jrc.ec.europa.eu/repository/bitstream/JRC107386/jrc_report_quantumcommunications.pdf

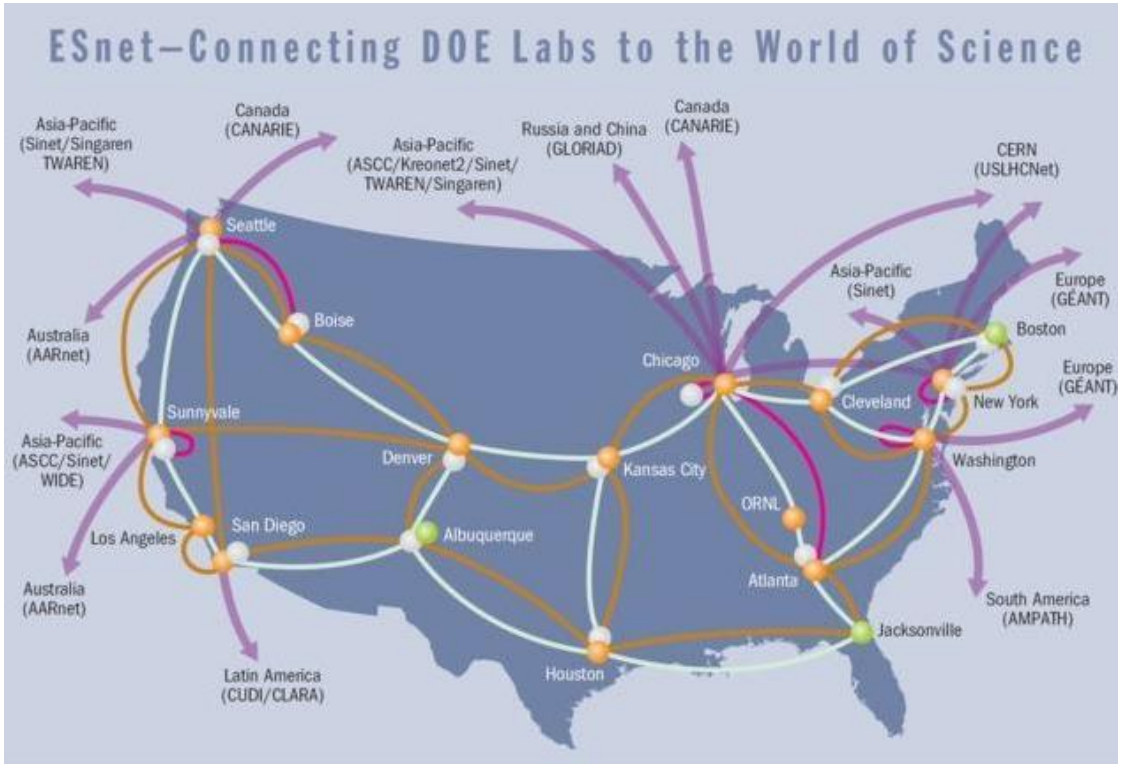


Fig. 27: The ESnet network operated by the DoE to interconnect critical scientific resources[71].

There are no official reports of QKD deployment in space by USA players. In 2017 the Chinese activism and the results obtained by the Micius satellite have been the object of a testimony for the US-China Economic and Security Review Commission at the US congress[72], and a Quantum National Initiative has been recently enacted[73]. In this context, NASA has laid out a vision and a roadmap for its quantum activities[74], see respectively Fig. 28 and Fig. 29.

[71] "Quantum Networks for Open Science Workshop", U.S. Department of Energy, Office of Advanced Scientific Computing Research, Rockville, Maryland, September 25 - 26, 2018; QNOS Workshop Final Report, March 2019, https://www.researchgate.net/publication/332041110_QNOS_Workshop_Final_Report

[72] "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

[73] **"**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-national-quantum-initiative-act/national-quantum-initiative-act-public-law-115-368

[74] Presentation by Barry Geldzahler (NASA Chief Scientist and Chief Technologist for Space Communication and Navigation) at the Toulouse Space Show on June 26, 2018 "NASA: Vision for Implementation of Quantum Communication".

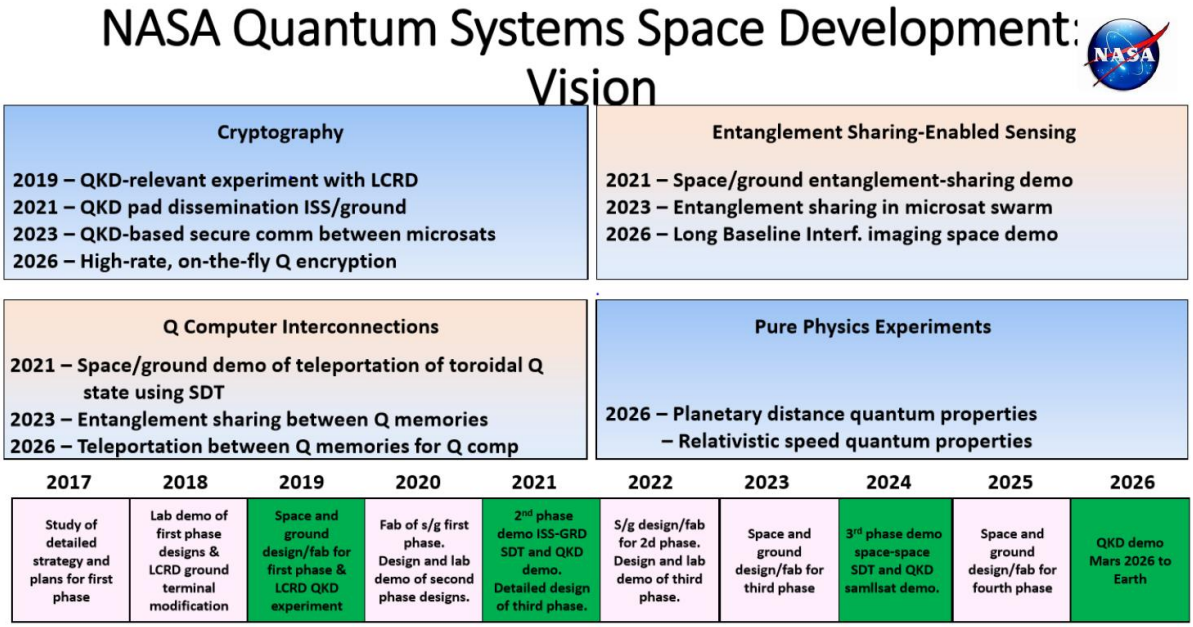


Fig. 28: Vision of NASA quantum activities

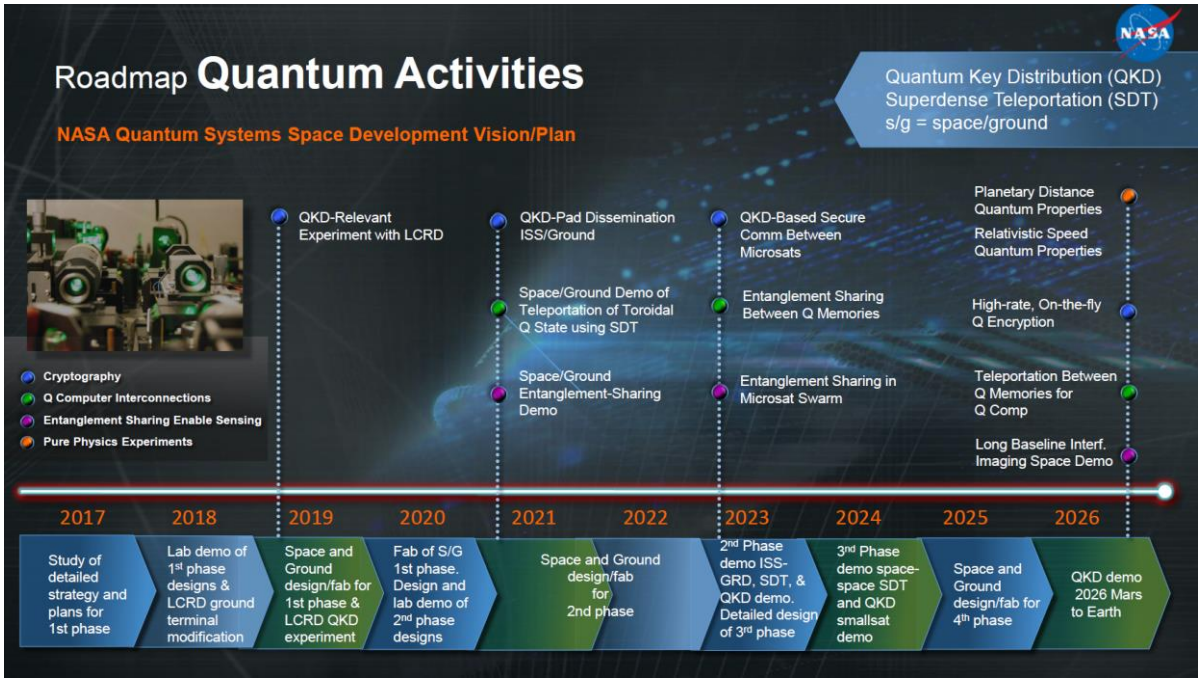


Fig. 29: roadmap of NASA quantum activities

For QKD in particular, several missions have been proposed:

- QKD from GEO to ground, using the Laser Communications Relay Demonstration
- QKD dissemination between the International Space Station and the ground
- Smallsat for QKD and QKD-based secure communications between microsatellites
- High-rate, on-the-fly Q-encryption
- QKD from a Mars orbiter to earth.

4.2 **Canada**

An overview of current efforts for development of quantum networks in Canada has been provided by a presentation given at a recent ITU event, see Fig. 30.

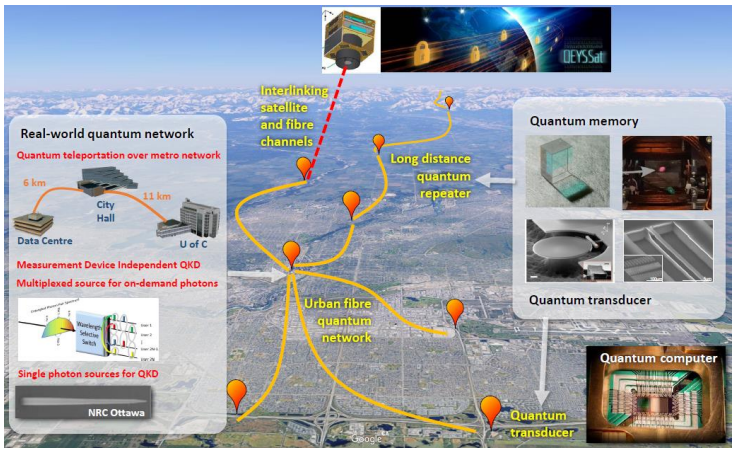


Fig. 30: Quantum communication network activities in Canada[75]

The University of Waterloo and the Institute for Quantum Computing (IQC) are working on a security analysis of practical QKD protocols, on quantum communications with coherent states, and on quantum repeater architectures. The University of Calgary is developing new protocols for coexisting classical and quantum communication. A MDI-QKD field test was carried out in 2013 in Calgary (see Fig. 31) over a total distance of 18.6 km with 9.0 dB loss, obtaining a secure key rate of ~1 bps[76], and a quantum teleportation experiment in a real-field deployment has been recently realised[77].

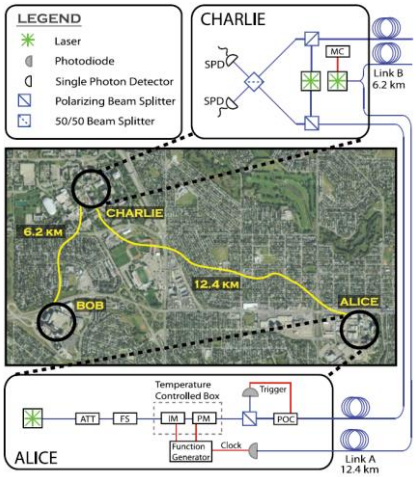


Fig. 31: QKD deployment in Calgary, used to test MDI-QKD. Alice and Bob are connected to Charlie by deployed dark fibres of 12.4 km and 6.2 km length, each of them with a ~4.5 dB loss.

---

[75] "Quantum Communication Network Activities Across Canada", ITU Workshop on Quantum Information Technology for Networks, Shanghai, June 2019, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Barry_Sanders_Presentation.pdf

[76] Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, Physical Review Letters, 111, 130501 (2013) https://physics.aps.org/featured-article-pdf/10.1103/PhysRevLett.111.130501

[77] "Quantum teleportation across a metropolitan fibre network", Nature Photonics volume 10, pages 676–680 (2016), https://arxiv.org/pdf/1605.08814.pdf

The University of Toronto is advancing twin-field QKD and reconfigurable multi-user QKD networks, and is developing broadband polarization entangled sources, see Fig. 32.

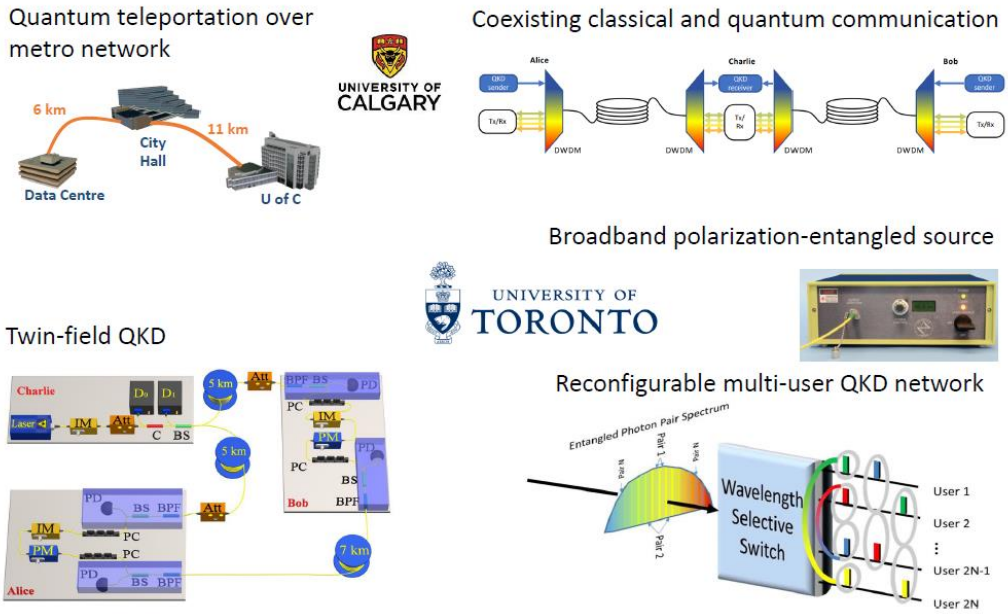


Fig. 32: experimental work on quantum networks at the Universities of Calgary and of Toronto

On the space side, the IQC team has been working to advance a proposed microsatellite mission called QEYSSat[78] through a series of technical studies funded initially by Defense Research and Development Canada and subsequently by the Canadian Space Agency. Its objectives are to demonstrate the generation of encryption keys through the creation of quantum links between ground and space, and to conduct investigations on long-distance quantum entanglement. IQC has also studied the feasibility of performing a rapid and low cost space-based QKD demonstration mission using a nanosatellite platform. In the autumn of 2016 the IQC team successfully demonstrated quantum key distribution (QKD) between a transmitter on the ground and a receiver payload on-board an aeroplane in the Ottawa area[79].

Finally, we mention the Quantum-Safe Canada not-for-profit organisation[80], which was established to "drive the efforts necessary to prepare for and respond to the quantum threat to encryption and cybersecurity, and to grasp the economic opportunities that exist in properly managing that threat".

[78] https://uwaterloo.ca/institute-for-quantum-computing/qeyssat

[79] "Airborne demonstration of a quantum key distribution receiver payload", Quantum Science and Technology, 2, 2, 024009 (2017), https://arxiv.org/pdf/1612.06396.pdf

[80] https://quantum-safe.ca/

5 Southern Africa

5.1 South Africa

A municipal quantum network was deployed in Durban under the QuantumCity project[81], consisting of four nodes connected in a star-configuration. Dedicated dark fibres have been used for the quantum links, with lengths varying between 2.6 km to 27 km, see Fig. 33[82]. ID Quantique QKD commercial equipment Cerberis has been used to feed primary AES session keys to commercial Senetas encryptors. This approach provided a layer-2 encryption to all passing traffic (data records, telephones, and internet). The system's overall performance has been stable during its ~4 month operational period: over a 2.6 km underground link, an average final secret key rate of 891 bps was achieved, then enhanced through layer-2 AES key expansion to allow for duplex communication between nodes at 1 Gbyte/s.

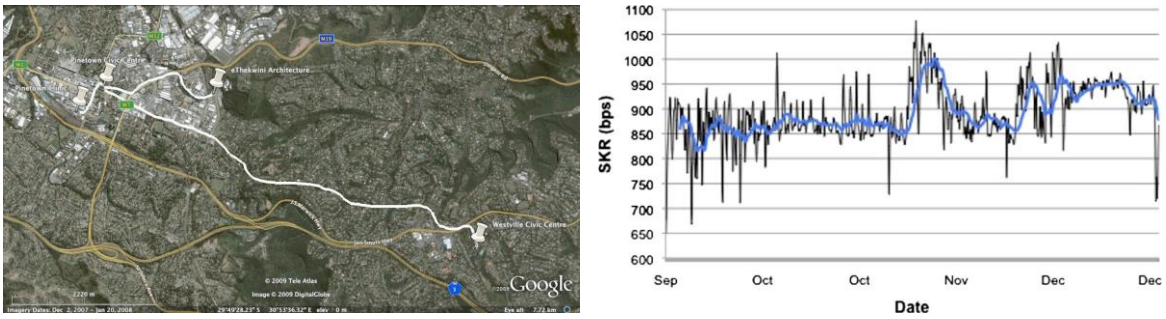


Fig. 33: map of the fibre layout in the QuantumCity project, and secure key rate over the testing period, September to December 2009.

[81] https://quantum.ukzn.ac.za/quantumcity/

[82] "Realizing long-term quantum cryptography", J. Opt. Soc. Am. B Vol. 27, No. 6, 2010 https://www.researchgate.net/publication/243580744_Realizing_long-term_quantum_cryptography

6 Summary Table

We summarise here the most important data characterising the performance of the deployments covered in this report. It may be immediately seen that the final secure key rate heavily depends on the link loss. Two caveats apply when comparing performances: the final secure key rate also depends on the choice of several operational security parameters; for lit fibre deployments, the performance also depends on the rate of the concurrent multiplexed classical data. Some types of system are inherently more costly or demanding in terms of the supporting infrastructure.

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
QuantumCtek QKD-PHA300 (commercial specs)	-	10 / 22	DF	DV	50 / 1
QuantumCtek QKD-POL1250 (commercial specs)	-	10 / 24	DF	DV	80 / 1
Hefei-Chaohu-Wuhu	85.1 69.7	18.4 14.1	DF	DV	0.77 0.8
Hefei metro	Several, 0.9 to 16.9	0.6 to 6.1	DF	DV	16 to 1
Wuhu metro	Several, 9 to 14.3	5 to 7	DF	DV	6 to 1
Zhucheng to Huangshan (Jinan-Qingdao)	66	~13	LF	DV	~3
Shanghai academic	Several, 2 to 40	3 to 15	LF	CV	10 to 0.25
Xi'an-Guangzhou	30 50	12.48 11.62	DF	DV	5.91 5.77
Hefei	17 25 30	5.1 9.2 8.1	DF	MDI	0.0388 0.0291 0.0165

Micius	LEO (500-1200)	~28 to ~33	Space	DV	1.1 (~300kb per pass)
Micius	1200 (between ground stations)	~65 to ~80	Space	Entanglement distribution	~1 photon per second
Tiangong-2	LEO 388 to 719	~32 to ~42	Space	DV	0.091 (~13kb per pass)
NEC-NICT	45	14.5	DF (with clock & sync)	DV	80
TREL	45	14.5	DF	DV	300
NTT-NICT	90	27	DF	DV	2.1
Mitsubishi	24	13	DF	DV	2
IDQ in Japan	13	11	DF	DV	0.3
Vienna team in Tokyo	1	1	DF	Entanglement	0.25
IDQ Cerberis[3] (commercial specs)	<50	12	DF	DV	1.4
Toshiba Tokyo 2015	45	14.5	DF	DV	300
Mitsubishi- Gakushin U.	10	7	DF	CV	50
Mitsubishi- Gakushin U.	10	7	LF	CV	27.2
Toshiba prototype (pre-commercial specs)	-	10	DF/LF	DV	Up to 1000
SK Telecom, Daejeon and Sejong	50	-	DF	DV	10
SECOQC: ID Quantique	25	5.75	DF	DV	1
SECOQC: TREL	33	7.5	DF	DV	3.1
SECOQC: GAP-IDQ-AIT	82	-	DF	DV	0.6
SECOC: Vienna-AIT-Kista	16	-	DF	Entanglement	2

SECOQC: CNRS-THALES-ULB	6.2	2.8	DF	CV	8
Swiss Quantum	3.7 14.4 17.1	2.5 4.6 5.3	DF DF DF	DV DV DV	2.4 0.9 0.9
Torino-Santhià	100	30	DF	DV	0.25
Florence	40	21	DF	DV	3.4
Sicily - Malta	96	22	DF	Entanglement	~0.06 (predicted)
Madrid - backbone	6	-	LF	DV	0.5
Madrid-GPON	3.5	-	LF	DV	0.02
Cambridge-Duxford	66	16	LF	DV	80
Cambridge-Telehouse	120	29	DF	DV	2
Cambridge metro	5.0 9.65 10.4	1.2 3.3 3.4	DF/LF	DV	3200/2900 3200/2700 2500/1400
Moscow	30	13	DF	DV	0.1
BBN-Harvard	10.2	5.1	DF	DV	1
Batelle Ohio	25	19	DF	DV	~1
Calgary	18.6	9	DF	MDI	0.001
Durban	2.6	-	DF	DV	0.9

Table I: QKD field deployments using optical fibre with prepare-and-measure protocols. DF: dark fibre; LF: Lit fibre; DV: discrete variable; CV: continuous variable; MDI: measurement-device-independent.

7 Conclusions

Today, one can say that a few tens of quantum key distribution systems at the 10 kilometre scale or greater have been deployed and successfully operated over a period of days or longer, in four continents and a dozen countries. A few examples exist of quantum networks at national scale, although none yet with anything approaching comprehensive coverage.

However, most of the deployments known rely on public funding. Only in a very limited number of cases has money comes from private development funding or potential customers investing to learn about a new technology. We have not identified an example of a deployment which is purely a private customer demanding the service for its immediate essential needs. The investments which have been made are with the intention of advancing and acquiring experience in a technology which is thought promising, even though its real future role remains unknown.

The most deployed quantum communications technology is discrete variable, prepare-and-measure QKD in dark fibre. Here the secure key rate can reach hundreds of kbps over links with ~10dB loss, enabling several applications. Significant progress has been made in multiplexing quantum signals in fibre also carrying classical data and there have also been several examples of continuous variable QKD deployments. MDI-QKD has been attempted in the field, and some examples of entanglement based QKD deployments can also be found. Another significant advance is the integration of QKD in modern optically switched, software-defined telecommunication networks. Deployments in space have also taken place, so far entirely reliant on public research funding.

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

List of abbreviations

AES	Advanced Encryption Standard
BB84	Bennett-Brassard 1984, a quantum communication protocol
BT	Formerly British Telecom, a company
CNR	Consiglio Nazionale delle Ricerche, Italy
CV	Continuous variable, a class of quantum communication protocols
COW	Coherent one way, a quantum communications protocol
DARPA	Defense Advanced Research Projects Agency, USA
DF	Dark Fibre
DV	Discrete variable, a class of quantum communication protocols
DWDM	Dense wavelength division multiplexed
EAL	Evaluation assurance level
ESA	European space agency
GEO	Geosynchronous Earth orbit
GPON	Gigahertz passive optical network
IQC	Institute of quantum computing, Canada
IDQ	ID Quantique SA, a company
INRiM	Istituto Nazionale di Ricerca Metrologica, Italy
ITMO	Information Technologies, Mechanics and Optics State University, Russia
ITU	International Telecommunication Union
JRC	Joint Research Centre of European Commission
LEO	Low earth orbit
LF	Lit Fibre
MDI	Measurement device independent
MEO	Medium Earth orbit
NDFIS	National dark fibre infrastructure service, UK
NICT	National Institute of Information and Communications Technology, Japan
NIST	National Institute of Standards and Technology, USA
NFD	Network function virtualization
OTP	One-time pad, cryptographic protocol
QCI	Quantum communications infrastructure
QKD	Quantum key distribution
QRNG	Quantum random number generator

SDN	Software defined network
SECOQC	Development of a global network for Secure Communication based on Quantum Cryptography, an EU project
TREL	Toshiba Research Europe Ltd.
VPN	Virtual private network
WDM	Wavelength division multiplexed

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications
You can download or order free and priced EU publications from EU Bookshop at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

KJ-NA-29865-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub

ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office of the European Union

doi:10.2760/38407

ISBN 978-92-76-11444-4