Future Quantum Networks: A Roadmap

Mohsen Razavi[1]

[1] *School of Electronic and Electrical Engineering, University of Leeds*

(Dated: 31 May 2021)

The prospect of deploying wide-scale quantum communications networks has received a considerable boost over the past decade. This is partly driven by several breakthroughs in the field, as well as its attracting substantial funding from governmental and industrial bodies. Different countries across the globe, including UK, Germany, Netherlands, and France, among others, in Europe, as well as China, Japan, and US have invested, on the order of several billion Euros overall, in their national quantum technologies programmes. European Union has also initiated an EU wide 10-year-long flagship programme of the same scale, to embrace and lead the second quantum revolution. Such investments have resulted in an accelerated progress in research and development of quantum technologies. Some of the examples in the quantum communications domain include:

- Intercity quantum networks, e.g., China's 2000-km-long Beijing-to-Shanghai link with over 30 network nodes; UK Quantum Network connecting several major sites across south of England; Netherlands' memory-based quantum network; and the EU wide prototype networks enabled by OpenQKD project;

- Satellite-based quantum communications enabled by the Chinese satellite Micius [1, 2] as well as several other initiatives that rely on cubesats [3];

- Implementation of several innovative quantum protocols that enable new applications, improve system performance, and/or resolve some security concerns [4–8], as well as the development of new theoretical techniques to support these innovations [9–14]; and

- Industrial uptake and wider outreach programmes to set the ground for wide-scale deployment of the technology.

In the context of above developments it is important to have a realistic view of how quantum technologies will evolve in the future, and in which directions we need to orchestrate our efforts. This roadmap document is going to address this subject from the viewpoint of deploying quantum key distribution (QKD) systems across our communications networks. This is where the expertise of our consortium is mainly focused on and also it best reflects the outcomes of the QCALL project. There have been several other recent roadmap documents that approach the question of future from different angles. Notably, the work in [15] adopts an application centric approach, whereas [16] focuses more on the required hardware. We believe this document complements the above efforts and altogether they offer a clearer picture of how quantum communications technologies can evolve over the next few decades.

QUANTUM KEY DISTRIBUTION NETWORKS

QKD has so far been one of the most successful applications of quantum technologies, which crucially addresses some security gaps in our current communications systems [17]. In particular, the threat from quantum computers being able to crack some of the widely deployed public-key cryptosystems has required developing new methodologies for sharing secret cryptographic keys among legitimate users. QKD offers a solution, based on laws of quantum mechanics, that offers forward secrecy, and, in that sense, it can be very useful in scenarios when data security is required over a long term. Examples of such scenarios include the exchange of medical records over the Internet, which, for privacy reasons, may need to be kept secure during the lifetime of an individual and even beyond that.

The original QKD protocols rely on the no-cloning theorem to encode the key bits onto single photons. While this is no longer a strict requirement [18], and there are also protocols that extract key bits from continuous variables obtained by measuring quadratures of an optical signal [19], it is still the case that, for security reasons, we are practically restricted to a-few-photon regime of operation. This would then impose limitations on the performance of the system, as measured by secret key generation rate, at long distances. In prepare-and-measure QKD protocols, the key rate often scales with the transmissivity of the channel. This turns out to be a fundamental bound for any repeaterless link [20]. Moreover, at sufficiently long distances, the noise in the channel/receiver would often dominate over the legitimate signals in which case secure exchange of keys would become impossible.

In order for QKD to be accessible to a wide range of customers it is essential to be deployed over long distances. Our envisaged solution for long-distance QKD is via multiple phases, which would naturally specify relevant milestones in our proposed roadmap; see Table I. Below, I explain what I would expect to be delivered in each phase, and what would be required to achieve it, with speculative timescales for relevant milestones.

Phase I: Trusted Node QKD Networks

The first phase of deployment, which is already underway, relies on trusted node QKD. In trusted node QKD, secret key exchange between parties A and B is done via multiple intermediate nodes located at sufficiently short distances from each other such that efficient point-to-point QKD is feasible between adjacent nodes; see Fig. 1. If these middle nodes can be trusted by parties A and B, then the exchanged key between adjacent nodes can be used to relay a key between A and B. If multiple independent paths exists between A and B, then the requirement on trusting the middle nodes can be alleviated.

From a technology development point of view, trusted node QKD, and all efforts dedicated to it, would certainly serve as a stepping stone toward future phases of deployment. This is why the

Stage of Development	Major milestones, services, or functionalities	Timeline (years)
Phase I: Trusted Node QKD Networks	Reliable chip-based QKD modules	0-5
	QKD standardisation for deployment on existing infrastructure	0-5
	Early demonstrations of additional satellite QKD links	0-5
	Adding QKD functionalities/modules to telecom networks	0-10
	Offering QKD services to private networks	0-10
	Offering QKD services via wireless optical links	0-10
Phase II: Partially Trusted QKD Networks	Upgrading telecom networks to support MDI protocols	5-10
	Upgrading telecom networks to support memory-enhanced protocols	5-10+
	Expanding satellite-based QKD and linking it to ground networks	5-10+
Phase III: Trust Free QKD Networks	Lab-based demonstrations of simple quantum repeater chains with no distillation	0-5
	Lab-based demonstrations of advanced quantum repeater chains with QEC-based distillation	5-10
	Field demonstrations of simple quantum repeater chains with no distillation	5-10
	Field demonstration of advanced quantum repeater chains with QEC-based distillation	10-15
	Adding repeater nodes in space	10-15+
	Upgrading telecom networks to support repeater nodes	10-15+

TABLE I. A possible roadmap, with speculative timelines, for deploying QKD technologies in our existing and developing infrastructure. The deployment can take place in three phases, where in each phase, by employing more advanced technologies, the trust requirement on the service provider nodes is reduced.

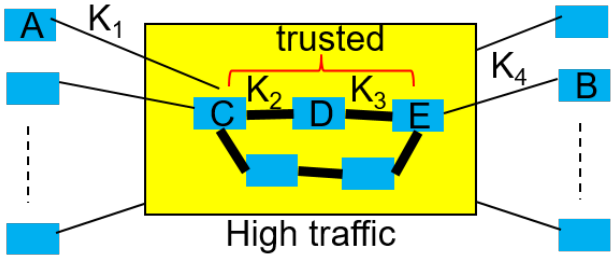

FIG. 1. The schematic of a trusted node QKD network. In order for users A and B to exchange a secret key, we need to create a secret key between any two adjacent nodes that connect A to B (e.g., C, D, and E). We can then use these keys to securely relay a key from A to B. If there are multiple paths between A and B, we can generate separate keys using each path and then combine them in the end.

trusted node QKD is at the core of almost all network demonstrations of QKD so far. This includes the Chinese backbone network, the EU OpenQKD networks, and the UK Quantum network, *inter alia*. This structure is expected to have certain niche markets among several sectors including military and government bases as well as the financial sector. While the assumption of all nodes being trusted may be acceptable in certain use cases, this is not necessarily the case in many other

scenarios that require end-to-end security. Despite this, looking into the future, the devices that we need to develop in this phase, such as chip-based QKD [21], efficient detectors and reliable sources, as well as learning how to manage resources over a hybrid communications network that supports quantum and classical applications, will all be useful and relevant in future phases of QKD deployment as well.

For all above reasons, we recognise the expansion of trusted node QKD as an essential part of the roadmap to QKD networks, and would expect that the next 10 years would be spent on improving the performance of its different components, as well as expanding the market within its relevant target sectors.

Phase II: Partially Trusted QKD Networks

The obvious follow-up to a trusted node QKD network is an upgraded network in which the trust requirement on middle nodes have been reduced so that a larger groups of customers are attracted to QKD services. There are several developing technologies that facilitate this transition:

- **Measurement-device independent (MDI) QKD:** MDI QKD enables two users to exchange a secret key via an untrusted node. This may only sound like a small adjustment to the trust issue, but, in practice, this will allow a larger number of enterprises to use the service as they can use the service provider nodes to connect two of their trusted nodes, see Fig. 2, and this way the need for having a fully private network would be alleviated. Moreover, with the new twin-field QKD protocols [7, 22, 23] on the rise, the MDI structure can be used to improve rate-versus-distance scaling as well. MDI protocols have been around for a while but have not yet been fully used in commercial settings. They pave the way for future phases of deployment.

- **Memory-assisted QKD:** An alternative way to improve rate versus distance scaling is to use quantum memories in the MDI setup [11, 24]. This will constitute the most primitive repeater system that relies on quantum memories, and will be the stepping stone to the solutions that need to be developed in the third phase. The first demonstrations of such systems have just been reported in literature [5, 6], and it will perhaps take some more time to see them implemented in realistic/commercial settings.

- **Satellite-based QKD:** one of the emerging routes to long-distance quantum communications is via satellites, possibly in different orbits, to serve as middle nodes between two ground stations. Prototype experiments of such nature has already been done using the Micius satellite exchanging a key between China and Austria by only trusting the satellite node [2]. Such a structure can also be expanded by using a constellation of satellites to serve

a large number of users [25]. It can also be used in the future to further expand quantum communications network of phase III to the space domain.

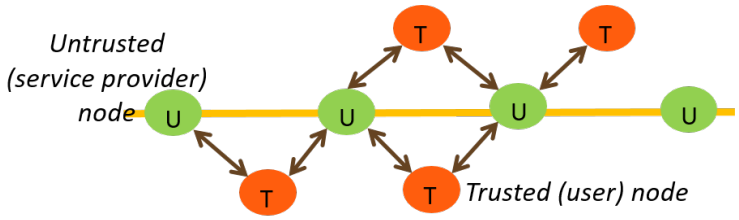

FIG. 2. The schematic of a partially trusted QKD network. We exchange a key, using, e.g., MDI techniques, between two adjacent trusted (T) nodes via the untrusted (U) node that connects them together. The key exchange between the two trusted nodes not directly linked via an untrusted node can then be done similar to that of Fig. 1.

It is envisaged that the above technologies can make substantial advances in the next decade or so, and will prepare us for the final phase of deployment when no trust on middle nodes of the network is needed.

Phase III: Trust Free QKD Networks

The key enabling idea behind trust-free QKD networks is to distribute entanglement between remote nodes in an efficient way. The users can then run an entanglement-based QKD protocol [26] to share a secret key while still being able to bound the amount of information that might have leaked to any potential eavesdropper. In effect, how the network provides the users with the entangled state does not matter from security assurance point of view, and, for that reason, the trust on middle nodes is no longer needed. An entanglement-based network can also accommodate many other quantum applications, e.g., distributed quantum computing, as reliable quantum data transfer can be achieved via quantum teleportation.

The conventional solution to efficient long-distance entanglement distribution is to use quantum repeaters [27]. Quantum repeaters extend the entanglement over a short distance to longer distances by employing certain joint measurements on quantum memories. The entangled state generated in this way may need to be distilled to obtain a higher quality entangled state. Based on the stage of development, the joint measurement and/or entanglement distillation can be done in either probabilistic [28, 29] or deterministic [30] ways. The probabilistic solutions often offer lower key rates and require longer storage times. The deterministic solutions, instead, require reliable quantum processing capabilities. Depending on the quality of quantum processing operations on the employed platform for our quantum repeater, we can then specify what services may be expected from our repeater-based network. In the long run, when high-performing quantum computers are available, we can in principle use quantum repeaters that do not require long storage

times, but, rather, encode the quantum data in large clusters of photons and send them from one node to another, where each node can correct for errors along the way and regenerate the encoded state [31].

The exact timing of commercial quantum repeaters of any form may be hard to predict, but we envisage some form of developments in 15+ years. The early demonstrations that rely on probabilistic measurements [32, 33] would continue to become more advanced in the next 15 years, while more efforts, aligned with progress in quantum processors, would also be directed in implementing quantum repeaters that rely on quantum error correction codes [34, 35]. A combination of such efforts, in addition to advancing our quantum memory units and their interaction with light [36], can bring us to the point where commercial deployment of quantum repeaters can become feasible in the forthcoming decades.

Within QCALL, we are delighted to have been able to do our part in advancing our field along the lines of this proposed roadmap. This can certainly continue by persistent investment in the field so that, one day, we can truly offer quantum communications services to all users.

---

[1] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43 (2017).

[2] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng-Zhi Li, Jian-Feng Wang, Yong-Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai-Le Liu, Franz Koidl, Peiyuan Wang, Yu-Ao Chen, Xiang-Bin Wang, Michael Steindorfer, Georg Kirchner, Chao-Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng-Zhi Peng, Jian-Yu Wang, Anton Zeilinger, and Jian-Wei Pan, "Satellite-Relayed Intercontinental Quantum Network," Phys. Rev. Lett. **120**, 030501 (2018).

[3] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling, "Advances in quantum teleportation," Nat. Commun. **3**, 30 (2017).

[4] R. I. Woodward, Y. S. Lo, M. Pittaluga, M. Minder, T. K. Paraïso, M. Lucamarini, Z. L. Yuan, and A. J. Shields, "Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers," npj Quantum Information **7**, 58 (2021).

[5] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, "Experimental demonstration of memory-enhanced quantum communication," Nature **580**, 60–64 (2020).

[6] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, "Quantum repeater node demonstrating unconditionally secure key distribution," Phys. Rev. Lett. **126**, 230506 (2021).

[7] Mirko Pittaluga, Mariella Minder, Marco Lucamarini, Mirko Sanzaro, Robert I. Woodward, Ming-Jun Li, Zhiliang Yuan, and Andrew J. Shields, "600-km repeater-like quantum communications with

dual-band stabilization," Nature Photonics **15**, 530–535 (2021).

[8] Massimiliano Proietti, Joseph Ho, Federico Grasselli, Peter Barrow, Mehul Malik, and Alessandro Fedrizzi, "Experimental quantum conference key agreement," Science Advances **7** (2021), 10.1126/sciadv.abe0395, https://advances.sciencemag.org/content/7/23/eabe0395.full.pdf.

[9] Hoi-Kwong Lo, Marcos Curty, and Bing Qi, "Measurement-device-independent quantum key distribution," Physical review letters **108**, 130503 (2012).

[10] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," Nature Communications **5**, 3732 (2014).

[11] Christiana Panayi, Mohsen Razavi, Xiongfeng Ma, and Norbert Lütkenhaus, "Memory-assisted measurement-device-independent quantum key distribution," New Journal of Physics **16**, 043005 (2014).

[12] Guillermo Currás Lorenzo and Mohsen Razavi, "Finite-key analysis for memory-assisted decoy-state quantum key distribution," New Journal of Physics **22**, 103005 (2020).

[13] Guillermo Currás-Lorenzo, Álvaro Navarrete, Koji Azuma, Go Kato, Marcos Curty, and Mohsen Razavi, "Tight finite-key security for twin-field quantum key distribution," npj Quantum Information **7**, 22 (2021).

[14] Gláucia Murta, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß, "Quantum conference key agreement: A review," Advanced Quantum Technologies **3**, 2000025 (2020), https://onlinelibrary.wiley.com/doi/pdf/10.1002/qute.202000025.

[15] Stephanie Wehner, David Elkouss, and Ronald Hanson, "Quantum internet: A vision for the road ahead," Science **362** (2018), 10.1126/science.aam9288, https://science.sciencemag.org/content/362/6412/eaam9288.full.pdf.

[16] David Awschalom, Karl K. Berggren, Hannes Bernien, Sunil Bhave, Lincoln D. Carr, Paul Davids, Sophia E. Economou, Dirk Englund, Andrei Faraon, Martin Fejer, Saikat Guha, Martin V. Gustafsson, Evelyn Hu, Liang Jiang, Jungsang Kim, Boris Korzh, Prem Kumar, Paul G. Kwiat, Marko Lončar, Mikhail D. Lukin, David A.B. Miller, Christopher Monroe, Sae Woo Nam, Prineha Narang, Jason S. Orcutt, Michael G. Raymer, Amir H. Safavi-Naeini, Maria Spiropulu, Kartik Srinivasan, Shuo Sun, Jelena Vučković, Edo Waks, Ronald Walsworth, Andrew M. Weiner, and Zheshen Zhang, "Development of quantum interconnects (quics) for next-generation information technologies," PRX Quantum **2**, 017002 (2021).

[17] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).

[18] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, "Practical decoy state for quantum key distribution," Physical Review A **72**, 012326 (2005).

[19] Frédéric Grosshans and Philippe Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).

[20] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi, "Fundamental limits of repeaterless quantum communications," Nature Communications **8**, 15043 (2017).

[21] Taofiq K. Paraïso, Innocenzo De Marco, Thomas Roger, Davide G. Marangon, James F. Dynes, Marco Lucamarini, Zhiliang Yuan, and Andrew J. Shields, "A modulator-free quantum key distribution

transmitter chip," npj Quantum Information **5**, 42 (2019).

[22] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).

[23] Jiu-Peng Chen, Chi Zhang, Yang Liu, Cong Jiang, Weijun Zhang, Xiao-Long Hu, Jian-Yu Guan, Zong-Wen Yu, Hai Xu, Jin Lin, Ming-Jun Li, Hao Chen, Hao Li, Lixing You, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," Phys. Rev. Lett. **124**, 070501 (2020).

[24] Silvestre Abruzzo, Hermann Kampermann, and Dagmar Bruß, "Measurement-device-independent quantum key distribution with quantum memories," Phys. Rev. A **89**, 012301 (2014).

[25] Carlo Liorni, Hermann Kampermann, and Dagmar Bruss, "Quantum repeaters in space," (2020), arXiv:2005.10146 [quant-ph].

[26] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557 (1992).

[27] H-J Briegel, Wolfgang Dür, Juan I Cirac, and Peter Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," Physical Review Letters **81**, 5932 (1998).

[28] W Dür, H-J Briegel, JI Cirac, and P Zoller, "Quantum repeaters based on entanglement purification," Physical Review A **59**, 169 (1999).

[29] L-M Duan, MD Lukin, J Ignacio Cirac, and Peter Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," Nature **414**, 413 (2001).

[30] Liang Jiang, Jacob M Taylor, Kae Nemoto, William J Munro, Rodney Van Meter, and Mikhail D Lukin, "Quantum repeater with encoding," Physical Review A **79**, 032325 (2009).

[31] William J Munro, Ashley M Stephens, Simon J Devitt, Keith A Harrison, and Kae Nemoto, "Quantum communication without the necessity of quantum memories," Nature Photonics **6**, 777 (2012).

[32] Yong Yu, Fei Ma, Xi-Yu Luo, Bo Jing, Peng-Fei Sun, Ren-Zhou Fang, Chao-Wei Yang, Hui Liu, Ming-Yang Zheng, Xiu-Ping Xie, *et al.*, "Entanglement of two quantum memories via fibres over dozens of kilometres," Nature **578**, 240–245 (2020).

[33] M. Pompili, S. L. N. Hermans, S. Baier, H. K. C. Beukers, P. C. Humphreys, R. N. Schouten, R. F. L. Vermeulen, M. J. Tiggelman, L. dos Santos Martins, B. Dirkse, S. Wehner, and R. Hanson, "Realization of a multinode quantum network of remote solid-state qubits," Science **372**, 259–264 (2021), https://science.sciencemag.org/content/372/6539/259.full.pdf.

[34] Yumang Jing, Daniel Alsina, and Mohsen Razavi, "Quantum key distribution over quantum repeaters with encoding: Using error detection as an effective postselection tool," Physical Review Applied **14**, 064037 (2020).

[35] Yumang Jing and Mohsen Razavi, "Simple efficient decoders for quantum key distribution over quantum repeaters with encoding," Phys. Rev. Applied **15**, 044027 (2021).

[36] Antonio Ortu, Alexey Tiranov, Sacha Welinski, Florian Fröwis, Nicolas Gisin, Alban Ferrier, Philippe Goldner, and Mikael Afzelius, "Simultaneous coherence enhancement of optical and microwave transitions in solid-state electronic spins," Nature Materials **17**, 671–675 (2018).