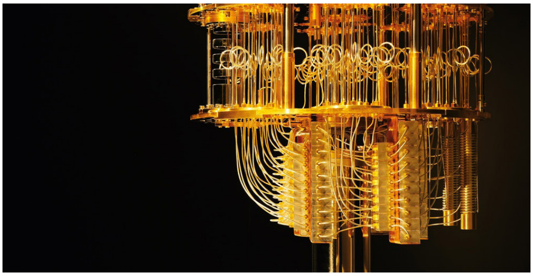
Drankadvies: Sapporo

Journey towards the quantum internet

Koji Azuma *Distinguished scientist, NTT Research Center for Theoretical Quantum Physics*

Information is described by utilizing differences of states of physical systems, while physical systems follow the laws of physics. Hence, the ultimate potential for information processing should be determined by such physics. This concept, given by renowned IBM fellow Rolf Landauer (1927-1999), is encapsulated in his famous proverbial statement 'Information is physical'. Nowadays, since the most precise and successful theory in physics is quantum mechanics (although it provides predictions far beyond our intuitions developed by our daily life or classical mechanics), the concept of Landauer can be interpreted as that the ultimate potential of information processing is determined by 'quantum mechanics' (beyond classical mechanics). In fact, this concept has triggered the finding of quantum computation and communication as our ultimate limit of information processing and has shown that we can accomplish information processing tasks that are intractable by conventional means. In this context a 'quantum internet' [1], a quantum version of the conventional Internet, may be an ultimate form of our information processing, given that the current internet is the biggest computer network on the Earth. Therefore it is important to understand, realize and expand the potential of a future quantum internet which would enable us to answer one of the most fundamental questions: what kind of information processing can be allowed by nature?



One of IBM's supercomputer models.

Possibilities of quantum internet

If you imagine the structure of the current internet, you would notice that it is composed of information processing nodes (such as computers and smart phones) and communication channels (such as optical fibres and free space) to connect them together. As a result, the internet enables arbitrary clients on Earth to communicate. Analogously, the quantum internet would be composed of 'quantum' information processing nodes (such as quantum computers) and 'quantum' channels (such as free space and optical fibres, as will appear later), which should enable arbitrary clients, independent of their spatial distances, to perform 'quantum' communication tasks in an efficient manner. Such a global quantum internet would have many applications [2]. For instance, the quantum internet would enable arbitrary users to perform information-theoretic secure communication using quantum key distribution (QKD) [3], even if eavesdroppers in the network are allowed to use universal quantum computers freely. This highly secure communication could be used for a referendum, a top-level meeting, a financial deal, an exchange of genetic/biological information and so on. Furthermore, the quantum internet enables any client to teleport unknown quantum states of their system to another [4], which is the basis of distributed quantum computing [5], quantum cloud computing [6,7], and ultimately, large-scale quantum computer networks.

Besides this, the quantum internet could be used for synchronizing atomic clocks with unprecedented stability and accuracy, in a completely secure manner [8]. It would also enable us to make baselines of telescope arrays unprecedentedly longer, contributing to the progress of astronomy [9]. Therefore, a worldwide race towards building up the quantum internet with these fascinating applications has now started. China has launched a satellite to achieve long-distance quantum communication and created a trusted relay QKD network over thousands of kilometres, the EU has started a project called the 'quantum internet alliance', and the US has just announced the preparation of a large budget (about 1.2 billion US dollars) for quantum technologies, called the 'US national quantum initiative' that will include research towards a future quantum internet.

Quantum internet in practice

How can we build up such a quantum internet in practice? The main role of the quantum internet is quite simple: it just needs to distribute 'quantum entanglement' for distributed clients in an efficient manner. The entanglement is a very peculiar correlation which can be held only by quantum systems and cannot be explained in the framework of classical mechanics or conventional probability/information theory. This entanglement was originally introduced by Podolsky, Einstein and Rosen to point out the (apparent) paradoxical nature of quantum mechanics [10]; ironically, it exists indeed and it is now known to be an extremely useful and even universal resource for achieving not only quantum communication but also quantum computation. Thus, we need to build up the physical layer for the quantum internet. This should be able to distribute such entanglement to clients, according to their requests, in an efficient manner.

An optical fibre network is regarded as a plausible candidate for the physical channel layer for the quantum internet, because optical fibres can efficiently deliver quantum information embedded into optical pulses and they are already installed in the world. Indeed, an optical fibre has already been used to perform point-to-point quantum communication in the form of the direct fibre transmission of photons between a sender and a receiver. The communication distance of this scheme has already reached about 400 km. However, it is considered that this communication distance cannot be more than that. This is because any optical fibre has photon loss which increases exponentially with its length. For instance, the success probabilities of transmission of a single photon, which is a typical quantum information carrier, over 50 km, 100 km, 150 km and 200 km optical fibres are approximately 10%, 1%, 0.1% and 0.01%, respectively. Therefore, for quantum communication over a 1000 km optical fibre, even with a GHz repetition rate, it would take over 100 years to obtain a unit of entanglement. This means that point-to-point direct quantum communication has a limitation on the achievable distance, which is not enough to achieve a global quantum internet. So how can we realize a quantum internet over an optical fibre network? The natural solution to this is to replace conventional repeaters with 'quantum' repeaters [11,12,13].

The global fiber optic network.

Use of quantum repeaters

The repeaters are used even in conventional communication networks to achieve long-distance communication against the photon loss of optical fibres. Here, the role of each repeater is to amplify (or measure and resend) signals of optical pulses which have been weakened by loss in the optical fibres. However, this mechanism cannot be used in quantum repeaters, because quantum signals cannot be amplified, owing to the no-cloning theorem [14] in the quantum world. Instead, 'quantum' repeaters generate entanglement between adjacent repeater nodes by exchanging photons through optical fibres. They transform, by their local operations, the established entanglement between adjacent repeater nodes into entanglement between a sender and a receiver as the resource for their quantum communication. This indirect establishment of entanglement with quantum repeaters has an exponential improvement over the point-to-point quantum communication in terms of communication efficiency, because quantum repeaters merely use optical fibres connecting adjacent repeater nodes, rather than ones connecting the sender and the receiver directly. Therefore, it is important to develop quantum repeaters.

The necessity and importance of quantum repeaters has also been proven by our recent theoretical progress on the understanding of the quantum/private capacity of lossy optical channel networks, where a lossy optical channel corresponds to the theoretical model of an optical fibre. The quantum (private) capacity gives the maximum obtainable entanglement (secret key) per use of given channels, by using arbitrary operations allowed in quantum mechanics. Therefore, it represents the true theoretical limit of the performance of quantum communication with given channels. Recently, excellent upper bounds on quantum and private capacity of point-to-point quantum communication over lossy optical channels (or optical fibres) have been derived [15,16]. Notably, these upper bounds have no scaling gap with 'existing' point-to-point quantum communication schemes, rendering the necessity of quantum repeaters for long-distance quantum communication conclusive. Subsequently, the upper bounds were generalized to have upper bounds on the quantum/private capacity of arbitrary lossy optical channel networks [17,18], beyond point-to-point communication. Besides, it was shown that the performance of running quantum repeater schemes between a sender and a receiver in a parallel manner, which is called aggregated quantum repeater scheme, achieves these upper bounds [19]. This concludes that the aggregated quantum repeater scheme accomplishes the quantum/private capacity of arbitrary lossy optical channel networks, irrespective of their topology, which implies that quantum repeaters must be a fundamental building block for the quantum internet. Therefore, even from a theoretical viewpoint, it is important for the quantum internet to develop quantum repeaters.

Realization of quantum repeaters

Now to realize quantum repeaters, we have two approaches [13]; one is to prepare quantum repeaters with matter quantum memories to store quantum information conveyed by photons; the other is to prepare quantum repeaters which work without quantum memory, towards a highest bandwidth quantum internet. In the first approach, we need to develop matter quantum memories which can efficiently entangle with photons and has a long coherence time (i.e., memory time). As candidates for this, atomic ensembles and a single qubit system (such as a nitrogen-vacancy (NV) centre in a diamond, an ion trap, a single atom and a quantum dot) are extensively studied both theoretically and experimentally. The second approach, which is relatively new, tries to develop information-processing matter qubits [20] or to sophisticate existing optical devices [21] (such as single-photon sources, linear optical elements, active-feedforward techniques and photon detectors), but it does not need quantum memories at all. Both approaches have different advantages, meaning that experimental progress along both approaches are important.

Our journey towards the quantum internet has just begun. In the near future, more fascinating applications of the quantum internet will be found, its potential will further be revealed and many experimental breakthroughs will occur. This progress must be because we are heading to the quantum internet as the Holy Grail of quantum information technology, consciously or even unconsciously.

I thank W. J. Munro for his helpful comments to write up this article. I also acknowledge the support, in part, from PRESTO, JST JPMJPR1861.

References

[1] Kimble, H. J. The quantum internet. Nature 453, 1023–1030 (2008).
[2] Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: A vision for the road ahead. Science 362, 6412 (2018).
[3] Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. Nat. Photon. 8, 595–604 (2014).
[4] Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 70, 1895–1898 (1993).
[5] Buhrman, H. & Röhrig, H. Distributed quantum computing. Rovan B., Vojtáš P. (eds) Mathematical Foundations of Computer Science 2003 (MFCS 2003), Lecture Notes in Computer Science 2747, 1-20 (Springer, Berlin, Heidelberg).
[6] Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. Proc. Of the 50th Annual Symposium on Foundations of Computer Science (FOCS'09), 517-526 (IEEE Computer Society, 2009).
[7] Aharonov, D., Ben-Or, M. & Eban, E. Interactive proofs for quantum computations. Proc. of Innovations in Computer Science (Beijing), 453-469 (Tsinghua University Press, 2010).
[8] Kómár et al. A quantum network of clocks. Nat. Phys. 10, 582 (2014).
[9] Gottesman, D., Jennewein, T. & Croke S. Longer-baseline telescopes using quantum repeaters. Phys. Rev. Lett. 109, 070503 (2012).
[10] Einstein, B. Podolsky, B. & Rosen N. Can quantum-mechanical description of physical reality be considered complete? Phys. Rev. 47, 777 (1935).
[11] Briegel, H. J., Dür, W., Cirac, J. I. & Zoller, P. Quantum repeaters: the role of imperfect local operations in quantum communication. Phys. Rev. Lett. 81, 5932–5935 (1998).
[12] Sangouard, N., Simon, C., de Riedmatten, N. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. Rev. Mod. Phys. 83, 33–80 (2011).
[13] Munro, W. J., Azuma, K., Tamaki, K. & Nemoto, K. Inside quantum repeaters. IEEE J. Sel. Top. Quant. Electron 21, 6400813 (2015).
[14] Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. Nature 299, 802–803 (1982).
[15] Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. Nat. Commun. 5, 5235 (2014).
[16] Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. Nat. Commun. 8, 15043 (2017).
[17] Azuma, K., Mizutani, A. & Lo, H.-K. Fundamental rate-loss trade-off for the quantum internet. Nat. Commun. 7, 13523 (2016).
[18] Pirandola, S. Capacities of repeater-assisted quantum communications. Preprint at http://arxiv.org/abs/1601.00966 (2016).
[19] Azuma, K. & Kato, G. Aggregating quantum repeaters for the quantum internet. Phys. Rev. A 96, 032332 (2017).
[20] Munro, W. J., Stephens, A. M., Devitt, S. J., Harrison, K. A. & Nemoto, K. Quantum communication without the necessity of quantum memories. Nat. Photonics 6, 777-781 (2012).
[21] Azuma, K., Tamaki, K. & Lo, H.-K. All-photonic quantum repeaters. Nat. Commun. 6, 6787 (2015).

Koji Azuma received his B.E., M.E., and Ph.D. degrees in physics from Osaka University, University of Tokyo and Osaka University, Japan, in 2005, 2007, and 2010 respectively. He joined NTT Basic Research Laboratories in 2010. His current interests are quantum information theory, especially for building the theory for a quantum internet. He was appointed as Distinguished Scientist of NTT in 2018. He is currently a member of Theoretical Quantum Physics Research Group. He is a member of the Physical Society of Japan. E-mail: *azuma.koji@lab.ntt.co.jp*