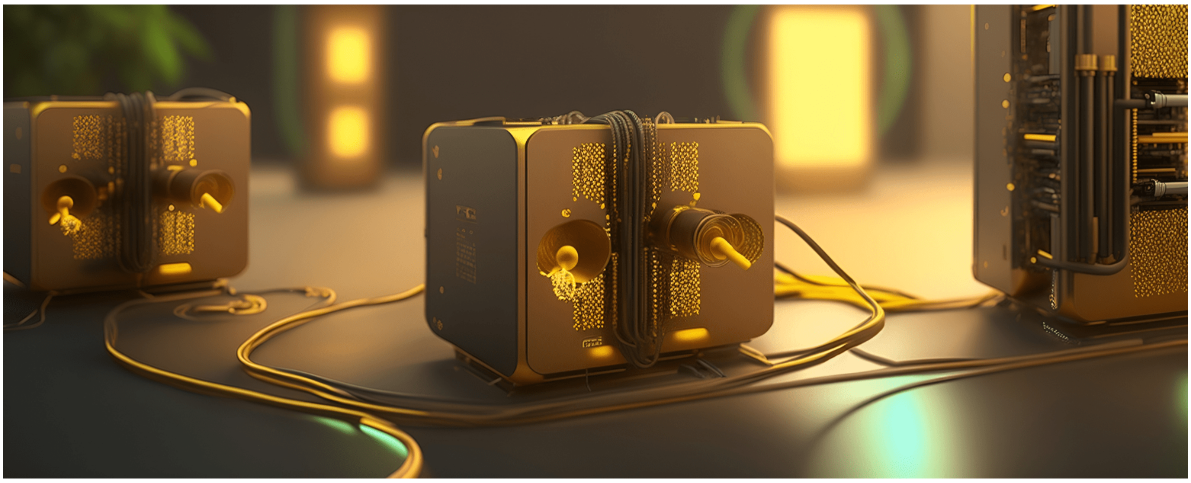
RESEARCH AND PRACTICAL APPLICATIONS

Quantum networks and Internet

Hugues de Riedmatten, Valerio Pruneri



Quantum physics and creative frequencies. Conceptualization: Luisa Quiroga

Communication is an essential element of our society. We all communicate with each other by sending information in the form of signals that can be easily generated and detected. For example, most of the data traffic that sustains the Internet today travels along optical fibres in the form of binary digits (bits) in sequences of zeros and ones known as bit strings. These bit strings are formed of pulses of photons – elementary particles of light – whose properties can be described with classical physics theory. Photons are ideal

Where a single photon is contained in a pulse, this becomes a quantum bit (qubit), a superposition of 0 and 1 quantum states whose behaviour is described with quantum mechanics theory. A fundamental property of qubits is that they cannot be measured without altering them, nor can they be cloned (copied). Two or more qubits can also form an entangled state, an ensemble of strongly correlated particles that influence each other even at a distance.

Superposition and entanglement are two fundamental quantum properties of quantum technologies, which include quantum communication, that is, the generation, transmission and detection of qubits. Similarly to today’s modern communication, quantum networks and internet, where the devices and systems are quantum, can be developed. Importantly, in most cases, the same fibre and satellite infrastructure over which classical bits currently travel can be shared, making global quantum networks and internet possible in the future.

First draft of the future secure quantum communication network

The quantum network and internet offers a significant number of unique functionalities and services which are not possible in classical communication [1]. Quantum cryptography, which we will describe in more detail further on, is probably the most advanced of these, and consists of distributing secret keys made of qubits (quantum keys) that are then used to encrypt and decrypt messages between two communicating parties. In practice, quantum cryptography combines quantum key distribution (QKD) and classical cryptography protocols to achieve secure communication which is impossible to hack, even with unlimited computational resources (e.g., quantum computers) and powerful algorithms. In June 2019, all 27 EU Member States agreed to build the European Quantum Communication Infrastructure (EuroQCI), a secure quantum communication infrastructure that will span the whole EU, including its overseas territories. In the last section of this paper we will present the initial plan to deploy the EuroQCI in the metropolitan area of Barcelona.

The maximal distance of quantum communication in optical fibres is limited to a few hundred kilometres, due to optical fibre loss and the fact that quantum bits cannot be amplified without adding noise that would prevent faithful communication. Quantum networks provide a solution to this problem by implementing quantum repeaters that combine entanglement distribution, and a device called quantum memory that enables the storage of entanglement in a material system. The realisation of quantum repeaters will allow fully quantum links over continental distances. However, many technical challenges will need to be overcome before a full quantum repeater can be implemented.

Besides QKD, several future applications have also proposed using the distribution of quantum entanglement over quantum networks, mostly in the areas of quantum computing and quantum metrology [1]. On the computing side, the first quantum computers will likely be large machines located in specific laboratories, similar to current supercomputers. The quantum internet would allow distant users to connect to these quantum computers in the cloud, securely and confidentially, in such a way that nobody – not even the quantum computer itself – would know what computation was being carried out. Another powerful futuristic application would be to bring quantum computers together. As each quantum computer has a limited number of qubits, connecting them via photonic links would enable access to a much larger number of qubits and therefore significantly increase the computational power. In addition to computing applications, future quantum networks may also find applications in quantum metrology. For example, it has been shown that networks of entangled optical clocks would enable more precise synchronisation. Similarly, it has been shown that building arrays of telescopes that share entangled states could raise their baseline, thereby increasing their sensitivity, which would lead to applications in astronomy.

> Quantum cryptography will allow to achieve secure communication which is impossible to hack, even with unlimited computational resources and powerful algorithms

The functionalities enabled by the quantum internet are fundamentally different to those of the classical internet, making the two types of network complementary. The quantum internet will not replace the classical one, but rather will complement it with new, previously impossible capabilities. Although several potential applications of the quantum internet already exist, it should be pointed out that most of the current applications enabled by the classical internet were not foreseen when early versions of the internet were developed. It is therefore reasonable to expect that a similar development will occur with the quantum internet, and that new applications will be discovered at the various stages of deployment.

Quantum cryptography

The security of current cryptographic schemes that protect the transmission of critical financial, health and governmental data is based on the difficulty of solving complex mathematical problems. The most widely used of these is the so-called RSA cryptographic protocol (after its inventors Rivest, Shamir and Adleman), whose security relies on the practical difficulty of factorising large numbers, and for which an efficient quantum factorisation algorithm was discovered by MIT Professor Peter Shor. The only reason that the RSA is still a viable encryption protocol today is that Shor’s algorithm requires a fault tolerant quantum computer to function; this technology, though not currently available, is rapidly evolving and is expected to become a reality in the coming decades. And when it does, the asymmetric key algorithms used over the Internet today will no longer be secure.

An alternative to counteract future attacks is to create algorithms and protocols that require the solution of problems not easily addressed by any computational technology. Post-quantum cryptography (PQC) algorithms, devised to provide computational security, are, in principle, not susceptible to currently known attacks performed with a quantum computer. PQC algorithms are expected to be able to operate as a software tool (with possible hardware acceleration), and the computational complexity for the trusted users (the resources required to encrypt and decrypt the message with the key) should be acceptable for the application of interest.

In contrast to algorithms offering computational security, QKD can provide information-theoretic security (ITS), that is, its security is demonstrated through solid mathematical proofs based on fundamental principles of quantum mechanics (e.g., the uncertainty principle and the no-cloning theorem), rather than the difficulty of solving certain problems. While the many variants of QKD may use different components, they are all based on the same scheme, involving two parties (Alice and Bob) that trust each other and wish to share a secret key they can use for future confidential communication. The secret key is transmitted by sending photonic qubits or entanglement between Alice and Bob via a quantum channel (e.g., an optical fibre) that connects them. If an eavesdropper (Eve) attacks the quantum channel, its parameters will inevitably be altered. Alice and Bob can quantify this alteration and this may guarantee that the final secret key is generated upon information unknown to Eve[2].

We note that perfect security is intrinsically impossible in realistic scenarios, but we can design systems, which, if implemented correctly, have a probability of failure against possible attack (even using future powerful quantum computers) that can be bound to a very small value, ϵ (of the order of 10-10 or smaller). For some cryptographic schemes, such as QKD, under certain conditions value ϵ is easy to calculate; in contrast, for systems that rely on computational security, mathematical progress could, in the worst case, destroy the security at any time and hence such a failure probability cannot be easily calculated. Besides, the probability of a successful attack against computationally secure primitives increases with time, as technological advances make more resources available to the attacker. This generates an unacceptable situation in applications that require long-term security. Flows of particularly sensitive information could be subject to “store now-attack later” attempts, where intruders capture encrypted information at certain moments in time with the hope of decrypting them in the future, when more powerful computational resources and/or algorithms are available.

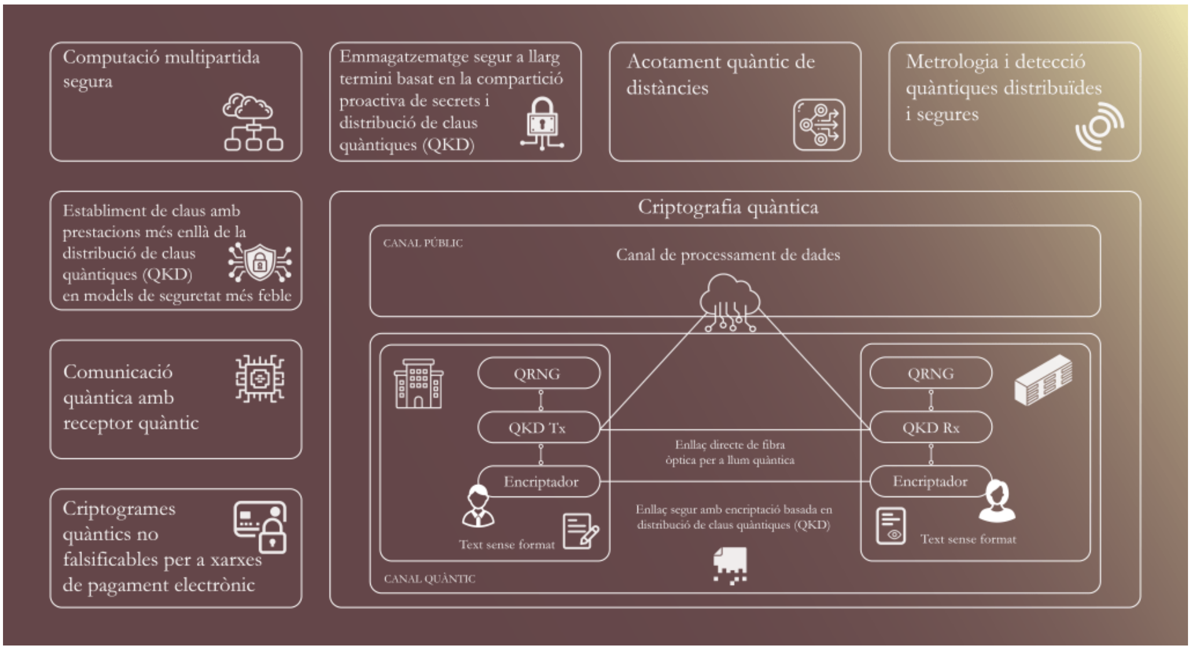

Computació multipartida segura
Emmagatzematge segur a llarg termini basat en la compartició proactiva de secrets i distribució de claus quàntiques (QKD)
Acotament quàntic de distàncies
Metrologia i detecció quàntiques distribuïdes i segures
Establiment de claus amb prestacions més enllà de la distribució de claus quàntiques (QKD) en models de seguretat més feble
Comunicació quàntica amb receptor quàntic
Criptogrames quàntics no falsificables per a xarxes de pagament electrònic
Criptografia quàntica
CANAL PÚBLIC
Canal de processament de dades
QRNG
QKD Tx
Encriptador
Text sense format
QRNG
QKD Rx
Encriptador
Text sense format
Enllaç directe de fibra òptica per a llum quàntica
Enllaç segur amb encriptació basada en distribució de claus quàntiques (QKD)
CANAL QUÀNTIC

Figure 1. Quantum cryptography: Ultra-secure communication can be achieved through quantum key distribution and encryption, while an additional range of applications, such as secure multiparty computation, secure long-term storage, and secure distributed sensing they can be implemented with quantum advantage in the network

Quantum cryptography is a rich area of research and applications that extend beyond QKD, e.g., secure multi-party computation, long-term secure storage (LTSS) based on proactive secret sharing and QKD, and secure distributed quantum metrology and sensing. While less mature than QKD, these applications have the potential to achieve quantum advantage in core networks.

Quantum memory and repeater

Quantum communication is usually achieved by sending photons through optical fibres over long distances. However, optical fibres suffer attenuation that scales exponentially with the distance. Even though standard optical fibre is one of the most transparent materials that exist, the loss becomes highly significant after a few tens of kilometres. For example, only 1% of the light is transmitted after 100 km of fibre, and only one part in 1020 after 1,000 km. In classical communication, this loss is compensated for by placing light-amplifying devices every 50 to 100 km along the installed fibre network. These amplifiers are what make the Internet as we know it possible, by allowing light to be transmitted through optical fibres over global distances. However, using such amplifiers is not an option in quantum communication, because qubits cannot be copied without adding noise to the quantum channel and rendering communication impossible. This limits practical quantum communications using optical fibres to a few hundred kilometres at most.

There are two solutions to this challenge. The first is to send photonic qubits through free space via satellites; quantum communication over more than 1,000 km has been demonstrated using this method. If, on the other hand, we wish to stay on the ground and use optical fibres, quantum repeaters have been proposed, using entanglement as the primary resource. The main idea of the quantum repeater is to split the total distance into several elementary links, generate entanglement independently between quantum nodes within each link, then extend the entanglement to more and more distant nodes by using a technique called entanglement swapping (see Figure 3). Once the entanglement has been distributed between distant nodes, it can be used for various tasks, such as quantum key distribution using entangled states, or the transmission of a qubit using a technique called quantum teleportation.

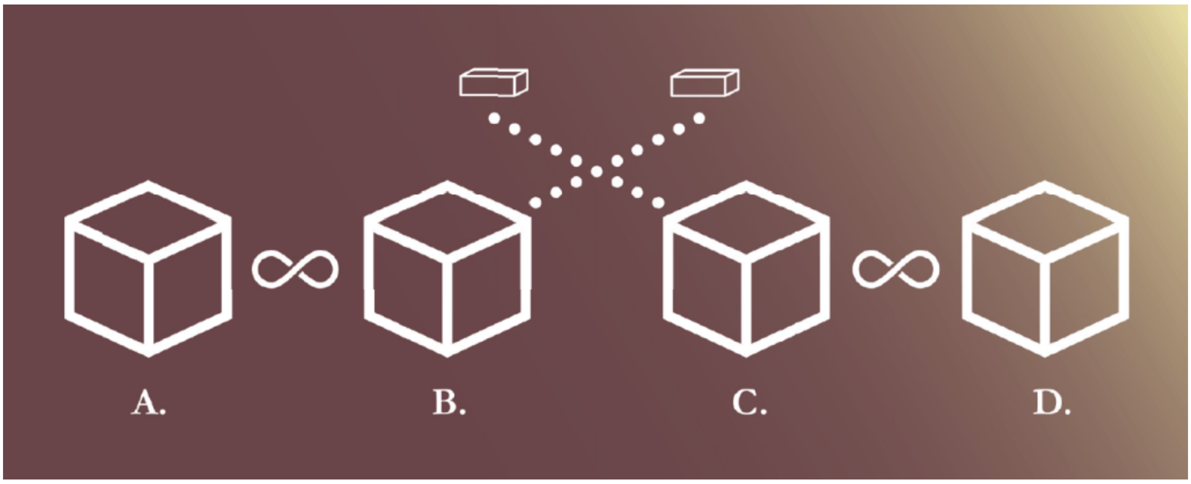


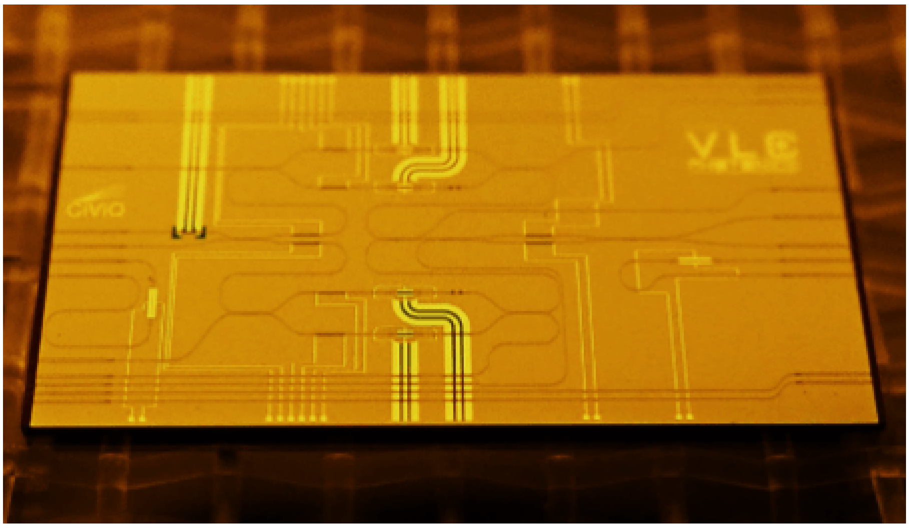
Figure 2. Architecture of the quantum repeater. The total distance is divided into different links. The entanglement is distributed independently on each link and stored in quantum memories. Once adjacent bonds are entangled, the distance is increased by entanglement exchange

A key building block for quantum repeaters is a device that allows the entanglement to be stored within one link until such time as other links are ready; this is referred to as a quantum memory. [3] Storing the entanglement allows the various elementary links to be entangled independently (i.e., they do not have to work simultaneously), which enables the distribution of entanglement at a rate that does not decrease exponentially with distance. Implementing a quantum memory for light usually requires coherent and strong interaction between single photons and some kind of atomic system whereby quantum information can be stored in long-lived atomic coherences. A number of physical systems are currently being explored, including cold atomic gases and solid-state systems based on rare-earth doped crystals. While important progress has been made in the last decade, building an efficient, long-lived and high-fidelity quantum memory capable of supporting a high level of multiplexing to enable a high rate of entanglement is still an outstanding experimental challenge and an active field of research. Beyond quantum memory devices, another challenge for quantum repeaters is to develop photonic entanglement sources suitable for interfacing with quantum memories, that is, that emit photons able to efficiently interact with the atomic memory system.

Building a functional quantum repeater that can transmit quantum entanglement over distances longer than those possible with direct transmission is a formidable experimental and technical challenge that will involve the efficient generation of high-fidelity entanglement between remote material systems, which in turn will require high-performance quantum nodes (combining quantum memory and entanglement source). In addition, the technology used must be robust and capable of being operated outside a controlled laboratory environment. All these challenges are currently being tackled under the auspices of a major European programme, the Quantum Internet Alliance, and it is expected that significant progress will be made in the next few years.

Miniaturisation and integration using photonic integrated circuits (PICs)

As with any new technology, for quantum networks and internet to achieve industrial and societal impact, a high level of miniaturisation and integration is mandatory. Integration enables the dimensions of the devices and systems providing the required functionalities to be reduced, thus reducing their power consumption and making large volume production of low-cost hardware possible. To simplify, two different levels of integration can be defined: (i) the technological level, whose objective is to miniaturise quantum communication subsystems into a combination of integrated photonic and electronic circuits; and (ii) the network level, involving the integration of quantum communication into the classical infrastructure, as well as the management software, large-scale deployment and upgradability of quantum networks and internet.



Integrated photonic circuit for the distribution of quantum keys developed through the CiViQ project

As for technology integration, such as electronic chips manipulating electron spins, photonic integrated circuits (PICs) allow miniaturisation thanks to the fact that photons, the primary carriers of the signals, are guided and processed in small dimensions. PICs are also allowing unprecedented performance to be achieved in quantum applications, for example, quantum random number generation, [4] QKD, entanglement sources, quantum memories and computation, to name a few. As a matter of fact, in information communication technologies using photons, an optoelectronic interconnection always exists, allowing electrical signals to be converted into photonic counterparts and vice versa. This means that electronic circuit boards (ECBs) are needed to perform the driving and reading out of PICs. Hardware for quantum networks and internet will therefore include PICs and ECBs, with optoelectronic integration playing an essential part. The hardware then requires a software interface that allows the end user to apply it in applications. [5]

As for network integration, to facilitate large-scale deployment the technology for quantum networks should be compatible with the existing fibre network infrastructure. [6] One important requirement is that the photons used to transmit quantum information must be at telecommunication wavelength, to minimise losses and permit the use of standard installed optical fibres. To allow the deployment of the quantum nodes in the field, in data centres, for example, the technology used should be compact, robust and reliable, and should operate in an automatised way, with minimal human intervention. To date, proof of principle demonstrations have been carried out in a controlled laboratory environment, and significant development is required to build deployable nodes. Finally, the quantum networks will need a dedicated software interface that makes the different components work together and allows users to use the network in a simple way, without knowing the details of the physical platform used. This is called a quantum network stack. A similar interface exists to access the classical internet but, since the quantum internet works in a radically different way, a specific network stack will be required and is currently being developed.

Barcelona Q-Network node

The European Commission and the European Space Agency are promoting and supporting the development of the EuroQCI), a pan-European quantum communication network composed of both terrestrial (fibre) and space (satellite) elements. In its initial phase, the EuroQCI is mainly focused on developing metropolitan nodes in major European cities, such as Barcelona; in the second phase, these metropolitan quantum nodes will be connected with each other.

Supported by projects sponsored by the Generalitat de Catalunya (SmartCAT, Qollserola, Qsunset, Qinfinity, Complementarias in quantum communication), the Spanish Ministry of Science and Innovation (Q-networks and Complementarias in quantum communication) and the European Commission (EuroQCI, QSNP, QIA), several quantum network architectures to demonstrate use cases of interest have been devised. As an example, Figure 5 shows a recent demonstration of a secure video call, based on QKD and quantum crypto, between two sites (CTTI and ICFO) located south of the Barcelona node.

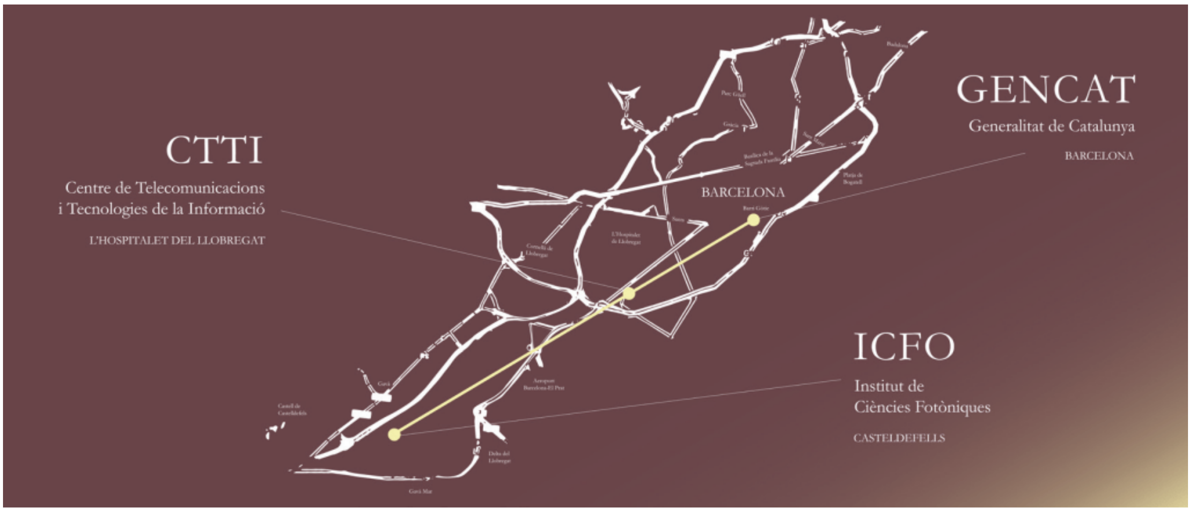


Figure 3. Demonstration in the Barcelona node of transmission of quantum key distribution (QKD) and secure video call between the CTTI and the ICFO using European-based technology: the continuous variable QKD system of the ICFO, technology developed in part under the CiViQ project and now transferred and produced by the new spin-off company Luxquanta and Quside's QRNG

As for technology, both superposition and entanglement resources will be used. This will include new devices and systems for quantum transmitters, receivers, memories and repeaters developed at research institutes in Catalunya, as well as counterparts produced by local (e.g., Quside and Luxquanta) and European companies with higher technology readiness levels. From a network architecture perspective, the BCN Q-network node will develop around Collserola tower, which is an ideal site to capture satellite quantum signals, transmit and receive free-space communication and connect to the core terrestrial fibre network of the metropolitan area. With critical inputs from Cellnex and other companies, quantum technologies and networks will be used to demonstrate use cases in the financial, health, transport and governmental sectors, to name but a few: secure transfer between two bank branches, for example, or transmission of health data between public hospitals and clinics will take place in the near future. The network will also be used to test quantum technologies for the next generation of fibre-based quantum networks using quantum repeaters and, further in the future, to implement connections between quantum sensors or computers.

REFERENCES AND FOOTNOTES

1 — S. Wehner, S., Elkouss, D., Hanson, R. (2018). Science 362, 6412.
2 — Bennett, C. H., G. Brassard, G., Ekert, A. K. (1992). Scientific American 267, 50–57.
3 — Afzelius, M., Gisin, N., de Riedmatten, H. (2015). Physics Today 68 (12), 42.
4 — Abellan, C., Amaya, W., Domenech, D., Muñoz, P. Capmany, J., Longhi, S., M. W. Mitchell, M. W., Pruneri, V. (2016). *Optica* 9, 989.
5 — Aldama, J., Sarmiento, S. López Grande, I. H., Signorini,, S., Trigo Vidarte, L., Pruneri, V. & Light, J. (2022) *Technol* 40, 7498.

6 — Lago-Rivera, D., Grandi, S., Rakonjac, J.V., Seri, A., de Riedmatten, H. (2021). Nature 594, 37.

Hugues de Riedmatten

Hugues de Riedmatten is an ICREA professor and head of the Quantum Photonics group at ICFO since 2010. His group's research focuses on building experimental hardware for quantum networks and quantum repeaters, including quantum memories for light, quantum light sources, quantum network nodes and quantum frequency conversion. He has a PhD from the University of Geneva in 2003, he is a member of the executive team of the European Quantum Internet Alliance. He contributed to key milestones in quantum repeater technology, including the first demonstrations of long-distance quantum teleportation, and of quantum repeater links using cold atoms and solid-state quantum memories.

Valerio Pruneri

Valerio Pruneri is an ICREA professor, president of the technological company specialized in materials Corning Inc. and head of group at the Institute of Photonic Sciences (ICFO). He has more than sixty patent families granted or pending, and has given a hundred lectures as a guest in the field of photonics and quantum technologies. Doctorate in 1996 from the University of Southampton, he currently coordinates the Quantum Secure Networks Association (QSNP) of the Quantum Flagship program of the European Commission. He is also coordinator of the EuroQCI Spain project of the European Quantum Communication Infrastructure. He has developed technologies for quantum random name generation and quantum key distribution, currently marketed by Quside and Luxquanta, respectively.