

# SPG MITTEILUNGEN COMMUNICATIONS DE LA SSP

## AUSZUG - EXTRAIT

### Progress in Physics (63)

**The challenge of long-distance quantum communication:  
From quantum repeaters to a quantum internet.**

*Mikael Afzelius, Department of Applied Physics, University of Geneva*

This article has been downloaded from:  
[https://www.sps.ch/fileadmin/articles-pdf/2018/Mitteilungen\\_Progress\\_63.pdf](https://www.sps.ch/fileadmin/articles-pdf/2018/Mitteilungen_Progress_63.pdf)

© see [https://www.sps.ch/bottom\\_menu/impressum/](https://www.sps.ch/bottom_menu/impressum/)

## Progress in Physics (63)

### The challenge of long-distance quantum communication: From quantum repeaters to a quantum internet.

*Mikael Afzelius, Department of Applied Physics, University of Geneva*

When most people connect to the internet through their tablets and smartphones, they might not know exactly what kind of technology makes the internet possible. But most physicists would know that at the physical network layer, internet data is composed of trains of short laser pulses zipping through optical fibres. The technologies underpinning the internet were developed during the second half of the 20<sup>th</sup> century, such as lasers, single-mode optical fibres, erbium-doped fibre amplifiers (EDFAs), electro-optic modulators and semiconductors, just to mention a few. As numerous technologies that are important for our society rely on the understanding of quantum mechanics, many refer to this as the first quantum revolution.

While the discovery of quantum mechanics was essential for the invention of lasers, transistors and other devices, in applications they do not explicitly exploit quantum effects such as superposition or entanglement. Across the internet, for example, classical bits of information are encoded using the amplitude or phase of the laser pulses consisting of large number of photons, where quantum effects are too weak and subtle to detect.

Today physicists work on novel quantum technologies that explicitly use quantum superposition and entanglement for their applications, with the goal of building devices that can outperform classical devices for secure communication, sensing, simulation and computation. Many therefore argue that we are in the beginning of a second quantum revolution, which might define many of the technologies to come in the 21<sup>st</sup> century. In Switzerland many research groups realized the potential of quantum technologies early on and the SNSF supports the NCCR "QSIT - Quantum Science and Technology" since 2011. On the European level a Flagship on Quantum Technologies is in the processes of being launched in 2018. At the same time large IT enterprises (Google, Intel, IBM, Microsoft) have started investing in quantum technologies. Here in Switzerland we recently saw ID Quantique, a spin-off company of our Department of Applied Physics at the University of Geneva that has commercially pioneered quantum cryptography, joining forces

with SK Telecom, the largest telecom operator in Korea. Clearly the recent gain in momentum for quantum technologies provides many exciting opportunities for researchers, students and engineers interested in quantum physics. The challenges are many as these new technologies are pushed upwards on the technological readiness ladder.

In this report I will focus on quantum communication over long distances, which has been identified as one of the key challenges for the coming decade. Today's systems for quantum cryptography, such as those from ID Quantique, are based on technologies that are fundamentally limited to distances up to maybe 500 km, while continental distances of 1000 km or more definitely will be out of range. To overcome this limit quantum repeaters have been proposed, in analogy to the classical repeater stations used in optical fibre communication. However, straightforward amplification of signals does not work in quantum communication, so quantum repeaters rely on entirely different principles. In fact, a quantum repeater will need a whole set of new technologies, such as quantum memories for single photons, sources of entangled photons, and very efficient single photon counters. Among these the most difficult part is often considered to be the quantum memory, which is the focus of my own research at the Department of Applied Physics at the University of Geneva. Future quantum repeaters will allow the distribution of quantum resources such as entanglement, with applications that go beyond quantum cryptography, e.g. for distributed computing or sensing applications, which lay at the heart of the vision of a quantum internet [1].

#### Quantum Key Distribution

The very first idea of a quantum communication protocol was published by Bennett and Brassard already in 1984 [2], who proposed a way to distribute a secret key between two parties where security can be guaranteed by the laws of quantum physics. So-called public key distribution is of even more importance now than back in 1984, as any secure communication over the internet (e.g. financial transactions) is based on public key distribution. The security of today's

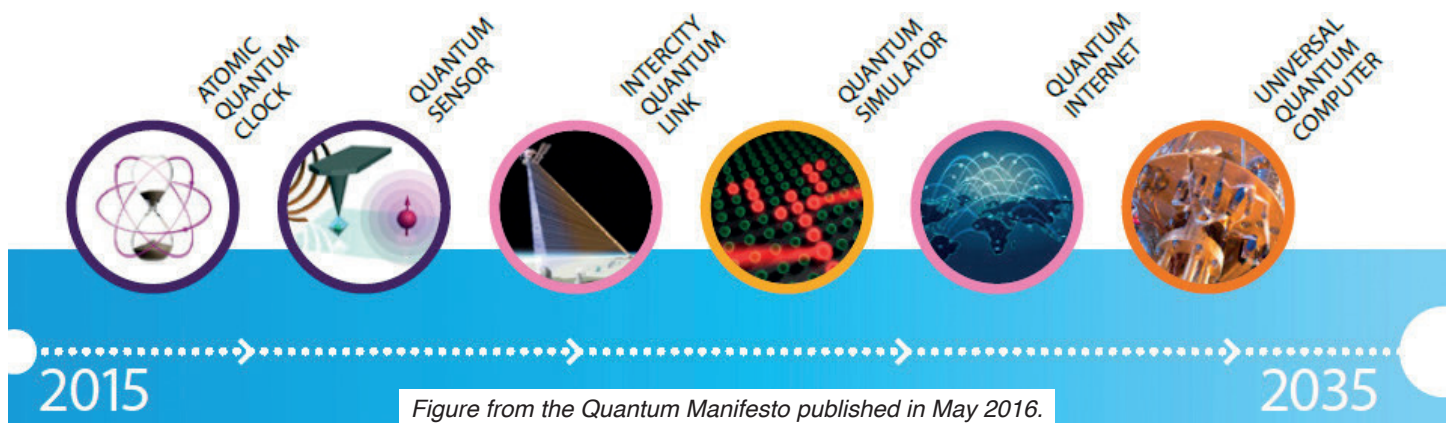


Figure from the Quantum Manifesto published in May 2016.

methods relies on mathematical problems that cannot be solved efficiently using known algorithms, but there is no guaranteed security with these methods. Also, a powerful quantum computer could break encrypted data in the future, meaning that very sensitive data communicated today might not be entirely secure in the future (we might want some secrets, such as medical records, to be hack-proofed also for the next decades!). Quantum key distribution (QKD) schemes provide a new paradigm, where security is guaranteed by the laws of quantum physics, whether it is now or decades in the future.

In classical communication, the information is encoded into bits, 0s or 1s, which can be represented by laser pulses with different amplitudes, for instance. In quantum communication, the information is encoded as qubits, which can be arbitrary superposition states  $\alpha|0\rangle + \beta|1\rangle$  of some basis states  $|0\rangle$  and  $|1\rangle$ . In short, the security of QKD is based on the fact that non-orthogonal qubit states, for instance  $|0\rangle$  and  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ , cannot be measured simultaneously. In a QKD scheme, the sender (Alice) and the receiver (Bob) randomly switch between non-orthogonal qubit states and measurement bases. Any adversary (Eve) that tries to spy on the communication, for instance by measuring some qubits, will necessarily modify some qubit states and introduce errors that are detectable by Alice and Bob. By measuring the so-called quantum bit error rate (QBER), Alice and Bob can guarantee that a provable secret key can be extracted from the measurement outcomes.

So how does one realize a QKD scheme in practice? On Alice's side the qubit is ideally encoded onto a single photon, because photons can travel far before losses become a problem. The qubit can be encoded into any degree of freedom, such as polarization, position or time(-bin). If the photon qubit will be sent through optical fibres then time-bin qubits are often used as they are more resilient to polarization rotation in fibres. In practice one can also replace the single-photon source on Alice's side by a laser pulse containing less than a photon in average (0.1 photons is commonly used), which is more practical than a true single-photon source. On Bob's side there is a qubit measurement device and a single-photon counter.

The challenges of current QKD research is to increase the quantum key rate and the maximal usable distance, which are very important for real-life applications. These two aspects are linked together, as the exponential losses of any channel, such as an optical fibre, implies that the photon detection rate is decreasing as the distance is increased. For both objectives, the performance of the detectors is determining. In the state-of-the-art QKD systems developed in the group of Prof. Hugo Zbinden at the University of Geneva, see Figure 1, the source qubit rate is 2.5 GHz and secret key rates of more than 1 kbit/s over 200 km of fibre can be achieved using simple semi-conductor detectors [3]. In order to further improve these performances, the Geneva group develops, in collaboration with colleagues from the University of Basel (Prof. Richard Warburton), superconducting single-photon detectors featuring more than 80% of detection efficiency and almost arbitrarily low noise [4]. With these detectors and ultra-low loss fibres, transmission distances of more than 400 km are expected, as well as

maximum secret key rates (over short distances) of up to 100Mb/s.

### The long-distance problem in QKD

The question is then how far one can transmit qubits with today's QKD systems? The photon transmission probability of any optical channel is exponentially decreasing with the distance. Commercial ultra-low loss optical fibres have loss coefficients of about 0.17 dB/km. If we assume a QKD system with an optimistic 10 GHz qubit rate, then the detection rate after 500 km is 31 Hz, which is still quite realistic for applications. But for a distance of 1000 km one would need to wait about 4 months to get a single photon detection!

In today's optical fibre networks, the loss problem is solved by inserting optical amplifiers at appropriate intervals, which amplify the laser pulses carrying the classical bits. In quantum communication this is not possible due to the no-cloning theorem [5], which says that an unknown quantum state cannot be amplified (cloned) without introducing errors. So, without the possibility to faithfully amplify qubits, it would look like QKD, or any other quantum communication scheme relying on sending qubits, is limited to about 500 km. But this is where quantum repeaters come in, as these can provide a solution to long-distance quantum communication in general, and specifically to long-distance QKD.

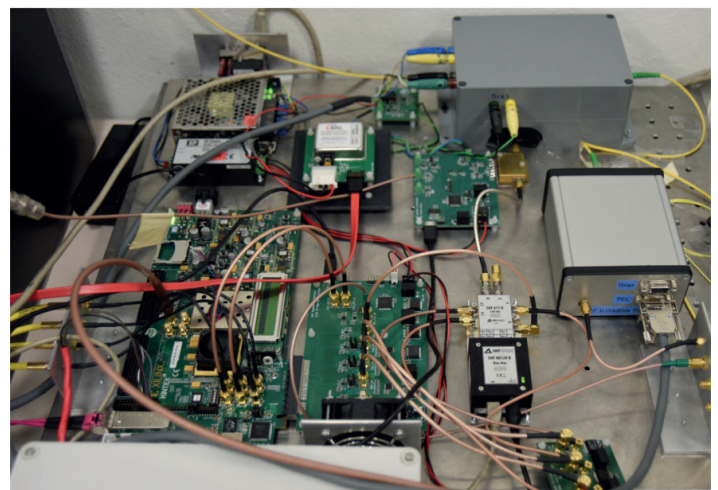


Figure 1. (Top) Commercial QKD system from ID Quantique based on a 2<sup>nd</sup> generation research prototype from University of Geneva. (Bottom) 3<sup>rd</sup> generation QKD prototype under development in the group of Prof. Hugo Zbinden at University of Geneva (courtesy Alberto Boaron).

But before describing the basic principles of quantum repeaters, I would like to mention the use of satellites for long-distance quantum communication. In 2016 China launched “Micius”, the first satellite dedicated to quantum science experiments. With “Micius” the group of Jian-Wei Pan demonstrated satellite-to-ground QKD up to distances of 1200 km [6]. These amazing experiments represent a real break-through for satellite-based QKD, but also reveal some of the limitations using satellites. The QKD downlink was only possible at night under good atmospheric conditions, and the low-altitude orbit implied that the satellite only briefly passed over the ground station during each orbit. But satellite communication could be the only option for some geographical situations, as crossing an ocean or a large mountain range. In my opinion future quantum networks will probably rely on both satellites and fibre-optic networks on the ground, as is the case for classical communication networks.

### Quantum Repeaters and Memories

The quantum repeater was first suggested by H.-J. Briegel et al. in 1998 [7], which is a method for overcoming the exponential loss-problem of point-to-point quantum communication. To understand how it works we need to have a basic notion of quantum entanglement, and the process of entanglement swapping. Let’s consider two photons  $A$  and  $B$  in an entangled state  $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|1\rangle_A|1\rangle_B + |0\rangle_A|0\rangle_B)$ . If Alice measures photon  $A$ , she would randomly obtain either the result 0 or 1, and so would Bob if he measured photon  $B$ . However, if they compare the measurement results they would make the astonishing discovery that their results are perfectly correlated, for some choices of measurement bases, although they could be space-like separated such that no signal traveling with the speed-of-light could explain this weird correlation (we say that the correlations are non-local). Entanglement, and the non-local correlations that it can produce, was for a long time considered as only interesting for the foundations of quantum mechanics, but has since then entered the realm of applied physics through the invention of quantum technologies.

In quantum communications the correlated measurement results obtained with entangled states can be used for quantum key distribution, as first proposed by Eckert in 1991 [8]. Shortly afterwards, in 1993, Bennet et al. realized that entanglement can also be used to perform so-called quantum teleportation [9], by which a qubit can be teleported from one place to another provided that an entangled state has

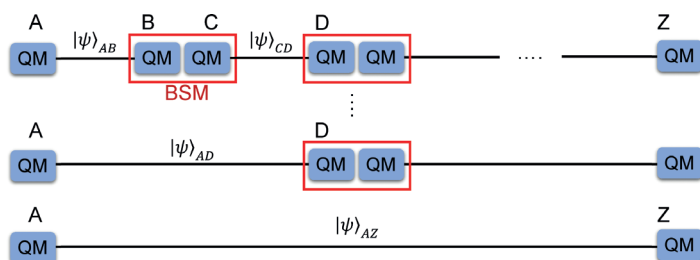


Figure 2. A quantum repeater breaks up the total distance between points  $A$  and  $Z$  into shorter elementary links. Entanglement between quantum memories (QM) in each node ( $A$  to  $Z$ ) is established independently using entangled photons. Entanglement swappings using Bell-state measurements (BSMs) then extend the entanglement to points  $A$  and  $Z$ .

been created between the two places. This discovery led others to propose a way to “connect” two entangled states through a process known as entanglement swapping. Let’s say we have two independent pairs of photons  $AB$  and  $CD$ , both in entangled states  $|\psi\rangle_{AB}$  and  $|\psi\rangle_{CD}$ . In entanglement swapping we perform a joint measurement on the photons  $B$  and  $C$ , a so-called Bell-state measurement (BSM), which projects photons  $A$  and  $D$  onto an entangled state  $|\psi\rangle_{AD}$  without them ever having interacted directly [10]! In fact, photons  $A$  and  $D$  could be 100s of km apart, as long as photons  $B$  and  $C$  are brought together to some measurement station where the BSM is performed.

This is the central concept behind quantum repeaters, as illustrated in Figure 2. If we want to entangle two systems (e.g. photons) over a very large distance, then we divide the total distance into shorter segments (elementary links) over which the losses are sufficiently low to be able to distribute entanglement (let’s say between 50 and 100 km). Once this step is done, one can perform BSMs on neighbouring entangled particles to swap the teleportation over ever larger distances, to end up with one final entangled state over let’s say 1000 km. Now, when using entangled photons the great difficulty is to succeed in the BSM. The photons have to travel large distances before reaching the BSM, meaning there is a significant probability of losing at least one of the photons, if not both. This is why we need quantum memories.

A quantum memory is a device that can store a single photon, effectively stopping it inside the memory, without destroying the quantum state that it carries. In most memories this is achieved by coherently mapping the quantum state carried by the photon onto a highly coherent atomic system, using some specifically engineered light-matter interaction. When we want to use the photon, we should be able to “push a button” to release it and use it, which usually means time-reversing the interaction process, as illustrated in Figure 3.

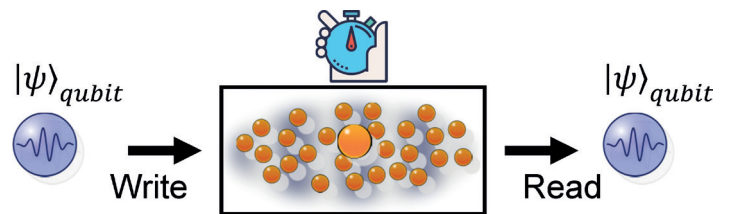


Figure 3. A quantum memory allows to write the qubit carried by a photon onto some material, here an ensemble of atoms or ions. After some variable time the memory can be read out, thereby creating an output photon carrying the same qubit state.

In the repeater, a quantum memory allows us to wait until two memories are charged with photons, before releasing both of them for the BSM. This ability is absolutely crucial in order for quantum repeaters to work over large distances. Please note that one doesn’t necessarily need to store the photon for very long durations, as in a classical memory (e.g. a hard drive). It is more like a buffer memory that allows us to temporarily store a photon. A quantum memory with a lifetime of about 1 seconds would already be very useful, but this is extremely challenging as the memory must then be able to preserve the quantum coherence during this time.

Several different physical systems have been considered as quantum memories for repeaters. In Switzerland a few groups work on these, including quantum dots [11] (Prof. Ataç İmamoğlu at ETH), atomic vapours [12] (Prof. Philipp Treutlein in Basel) and rare-earth (RE) ion doped crystals (our group at the University of Geneva) [13,14]. It would be out of the scope of this report to discuss them all, I will therefore only mention a few important results that we have achieved recently using RE crystals.

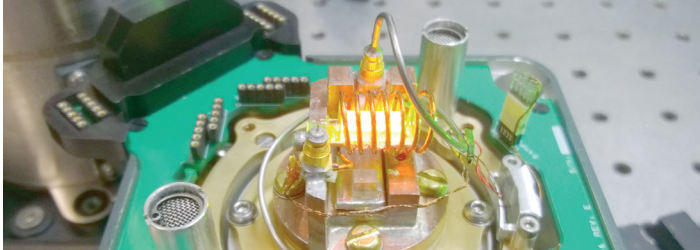


Figure 4. A quantum memory based on a Europium-doped crystal. The crystal is mounted inside a closed-cycle cryostat that cools it to about 3 K. Multiple photonic qubits can be stored inside this crystal for durations of up to one millisecond.

Quantum memories based on RE crystals, see Figure 4, have several appealing properties for quantum memories, of which maybe two stand out; long coherence times (i.e. long memory times) and the ability to store many photonic qubits in one device (multiplexing). Just as in classical networks multiplexing means higher rates, and it has been shown that multiplexing is crucial for long-distance quantum repeaters. However, it has proven very challenging to store more than one qubit in any quantum memory. In 2008 colleagues and I proposed a new quantum memory scheme that has the highest multiplexing capability [13], specifically when used in conjunction with RE crystals. Using this scheme we were able to store five polarization qubits inside a RE crystal for up to about 1 ms [14], see Figure 5, a significant improvement for quantum memories based on solid-state materials. In a more recent experiment we could show that the memory can store quantum correlations on the same time scale [15], which is a key requirement for repeaters. But many challenges remain, such as improving the memory efficiency, and further increasing the memory lifetime and multiplexing ability. In particular these key properties must be improved simultaneously in one memory device, which is a challenge for all the different approaches to quantum memories. For readers especially interested in quantum memories I refer to the following *Physic Today* feature article that colleagues and I wrote in 2015 [16].

## The Quantum Internet

A quantum repeater uses entanglement as its key resource, meaning that it can be used for much more than conventional QKD. Entanglement-based quantum communication allows so-called device independent schemes, for QKD, random-number generation and other applications, where security can be guaranteed by the user without even trusting the device manufacturer. A repeater could also be used to teleport a quantum state over a very large distance. In a proof-of-principle experiment we recently demonstrated this by teleporting a polarization qubit from a telecom photon into a quantum memory [17]. Building on such experiments

one could imagine to connect smaller quantum computers using repeater links, to realize a larger, more powerful, distributed quantum computer [1]. It could also allow a user to connect to a powerful quantum computer and perform the computation without its owner having any knowledge about the results (blind quantum computing). The possibilities of a network of quantum processors connected through a repeater network are many, and some of them we probably can't even imagine now. It is therefore important to get a larger part of the society involved in this endeavour, if we truly are to unlock the potential of quantum technologies.

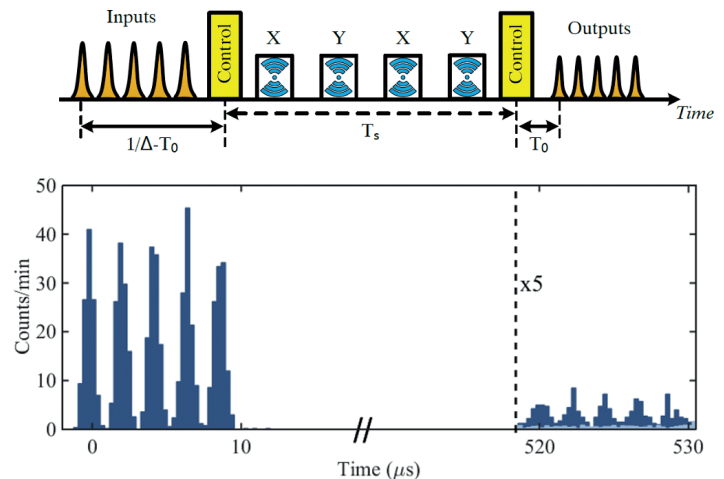


Figure 5. (Top) Illustration of the sequence of input and output pulses (orange), optical (yellow) and radio-frequency (blue) control pulses used in a quantum memory experiment. The intense control pulses coherently maps the input pulses into the memory, and assures the mapping back into the output pulses. (Bottom) Experimental photon counting histogram showing five input and output pulses, which are stored for about 0.5 ms. Each input pulse contains about two photons in average.

- [1] H. J. Kimble, *Nature* **453**, 1023 (2008).
- [2] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, **175** (Dec. 1984).
- [3] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin and H. Zbinden, *Appl. Phys. Lett.* **112**, 171108 (2018).
- [4] M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schenberger, R. J. Warburton, H. Zbinden and F. Bussiès, *Appl. Phys. Lett.* **112**, 061103 (2018).
- [5] W. K. Wootters and W. H. Zurek, *Nature* **299**, 802 (1982)
- [6] S.-K. Liao et al., *Nature* **549**, 43 (2017).
- [7] H.-J. Briegel, W. Dür, J. I. Cirac and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).
- [8] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [9] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [10] M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon and H. Zbinden, *Nat. Phys.* **3**, 692 (2007).
- [11] A. Delteil, Z. Sun, W.-B. Gao, E. Togan, S. Faelt and A. İmamoğlu, *Nat. Physics* **12**, 218 (2016)
- [12] J. Wolters, G. Buser, A. Horsley, L. Béguin, A. Jöckel, J.-P. Jahn, R. J. Warburton and P. Treutlein, *Phys. Rev. Lett.* **119**, 060502 (2017)
- [13] M. Afzelius, C. Simon, H. de Riedmatten and N. Gisin, *Phys. Rev. A* **79**, 052329 (2009).
- [14] P. Jobez, C. Laplane, N. Timoney, N. Gisin, A. Ferrier, P. Goldner and M. Afzelius, *Phys. Rev. Lett.* **114**, 230502 (2015).
- [15] C. Laplane, P. Jobez, J. Etesse, N. Gisin and M. Afzelius, *Phys. Rev. Lett.* **118**, 210501 (2017).
- [16] M. Afzelius, H. de Riedmatten and N. Gisin, *Physics Today* **68**, 12, 42 (2015).
- [17] F. Bussiès, C. Clausen, A. Tiranov, B. Korzh, V. B. Verma, S. W. Nam, F. Marsili, A. Ferrier, P. Goldner, H. Herrmann, C. Silberhorn, W. Sohler, M. Afzelius and N. Gisin, *Nat. Photon.* **8**, 775 (2014).