npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Proposal for space-borne quantum memories for global quantum networking

Mustafa Gündoğan[1]✉, Jasminder S. Sidhu[2], Victoria Henderson[1], Luca Mazzarella[2], Janik Wolters[3,4], Daniel K. L. Oi[2] and Markus Krutzik[1]

Global-scale quantum communication links will form the backbone of the quantum internet. However, exponential loss in optical fibres precludes any realistic application beyond few hundred kilometres. Quantum repeaters and space-based systems offer solutions to overcome this limitation. Here, we analyse the use of quantum memory (QM)-equipped satellites for quantum communication focussing on global range repeaters and memory-assisted (MA-) QKD, where QMs help increase the key rate by synchronising otherwise probabilistic detection events. We demonstrate that satellites equipped with QMs provide three orders of magnitude faster entanglement distribution rates than existing protocols based on fibre-based repeaters or space systems without QMs. We analyse how entanglement distribution performance depends on memory characteristics, determine benchmarks to assess the performance of different tasks and propose various architectures for light-matter interfaces. Our work provides a roadmap to realise unconditionally secure quantum communications over global distances with near-term technologies.

npj Quantum Information (2021)7:128 ; https://doi.org/10.1038/s41534-021-00460-9

INTRODUCTION

Quantum technologies such as quantum computing[1,2], communication[3,4] and sensing[5–7] offer improved performance or new capabilities over their classical counterparts. Networking, whether for distributed computation or sensing can greatly enhance their functionality and power. As one of the first applications of quantum communication, quantum key distribution (QKD) has been leading the emergence of quantum information technologies and establishes the foundation for wide-scale quantum networking[8]. In QKD, the security of secret keys shared between two parties are guaranteed by the law of physics and not only through the computational power of an adversary. The last three decades have seen significant progress in QKD enabling technologies including hand-held devices[9], integrated optics fabrication[10] and photon detectors[11].

However, the main limitation to current implementations is the range over which a secure link can be established. Ground-based QKD systems are inherently limited by in-fibre optical losses, specifically, the key generation rate decreases exponentially with distance[12,13]. By using cryogenically-cooled superconducting nanowire single-photon detectors (SNSPDs), Boaron et al. have demonstrated the secret key distribution of around 6 Hz at a distance of 405 km[11]. More recent twin-field QKD[14] methods have pushed this limit beyond 500 km[15]. Both of these demonstrations have utilised state-of-the-art ultra-low loss optical fibres, with losses around 0.17 dB/km, with further improvements unlikely in a medium time horizon.

Conventional optical repeaters cannot be used with QKD as quantum information cannot be deterministically cloned[16]. This provides unconditional security against eavesdropping. Current long-distance fibre QKD links employ trusted nodes that effectively relay a secure key between the end points. Trusted nodes are assumed to be safe from malicious parties and are potential points of weakness. Trusted nodes are also unsuitable for the long-range distribution of entanglement, hence the need to overcome the terrestrial limits (~1000 km) of direct quantum transmission.

Moving beyond these limits requires the use of intermediate nodes equipped with quantum memories (QMs) or quantum repeaters (QRs), which do not need to be assumed free from malicious control (untrusted operation). By exploiting the assistance of QRs to divide the transmission link into smaller segments, it is possible to overcome the fundamental rate-loss scaling for direct transmission, though at the expense of many intermediate repeater nodes (one every <100 km) that could be costly and difficult to construct. QRs perform local entanglement swapping operations to distribute entanglement across the whole link[17,18]. The use of repeater chains naturalise transmission links to arbitrary quantum networks that can be analysed and simulated using deep results from the classical network theory[19]. Current fibre-based QRs are still limited to around ~4000 km[20] beyond which generation of meaningful key rates (i.e. ~1 Hz) becomes extremely challenging due to the need for a large number of repeater stations. This falls short for a solution to global or intercontinental scale quantum communications.

The use of satellites may also extend QKD beyond the terrestrial direct transmission limit and is a natural approach to join different intercontinental fibre networks. Terrestrial free-space QKD is ultimately range limited by the Earth's curvature and the method is suitable mainly for intra- and inter-city links[21]. In satellite QKD (SatQKD)[22–25], the transmission loss through the vacuum of space is dominated by diffraction that has an inverse square scaling instead of exponential. However, the connection distance for SatQKD is primarily limited by the line-of-sight between satellite and ground station, which in turn depends on its orbit unless the satellite acts as a trusted node[26–30]. To establish a global quantum network without trusted nodes will require overcoming the above

[1]Institüt für Physik, Humboldt-Universität zu Berlin, Berlin, Germany. [2]SUPA Department of Physics, University of Strathclyde, Glasgow, UK. [3]Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR), Institute of Optical Sensor Systems, Berlin, Germany. [4]Technische Universität Berlin, Institut für Optik und Atomare Physik, Berlin, Germany. ✉email: mustafa.guendogan@physik.hu-berlin.de

limitations. The use of quantum satellites equipped with QMs as QRs remains relatively unexplored.

In this paper, we develop and characterise a new approach for global quantum networking using space and ground networks. Our approach exploits satellites equipped with QMs to provide free-space optical repeater links to connect two end stations on the ground. We implement MA measurement-device independent QKD (MA-QKD) protocols[31–33] to achieve high rates and device-independent security on board satellites in a line-of-sight setting. This is the first detailed quantitative analysis of QMs aboard satellites. The entanglement distribution rate is used as a benchmark to assess the performance of our repeater chain. Our approach overcomes limitations in purely ground-based repeater networks and trusted satellite relays to outperform previous quantum MA-QKD studies and provide the current best rate-loss scaling for quantum communications over planetary scales. Notably, we demonstrate that satellites equipped with QMs provide three orders of magnitude faster entanglement distribution rates over global distances than existing protocols. For connecting ground-based networks, we show that QMs can increase key rates for general line-of-sight distance QKD protocols.

We exemplify this by analysing a Vienna-Sydney link that is separated by nine ground stations, complete with weather effects. This additional analysis improves our result significantly. The inclusion of a good weather probability at each ground station renders previous hybrid repeater schemes impractical by comparison and highlights the importance of adopting QMs on board satellites. We also investigate the impact of losses from the operation of the QMs. Our work provides a practical roadmap towards the implementation of global communication, navigation and positioning and sensing. It also provides the means to benchmark the noise that can be tolerated in different scenarios as a function of the channel loss. We conclude by discussing several QM platforms for space-based quantum repeater and MA-QKD protocols.

RESULTS

Here we first outline and present results for two QR protocols for global entanglement distribution. This will be followed by MA-QKD protocols in uplink and downlink configurations to increase the key rates in quantum communication within the line-of-sight distance. Here the QMs are used as quantum storage devices to increase the rate of otherwise probabilistic Bell state measurements (BSMs) that form the backbone of most MDI protocols. We compare these results with known results that use ground-based and hybrid schemes. We focus on low Earth orbit (LEO) to directly compare our results with existing experimental demonstrations. This analysis is extended to geostationary orbits in supplementary materials in the context of global quantum repeater architectures.

Quantum repeaters

QRs can be grouped into different architectures depending on the error correction mechanism employed[18]. The first generation of QRs rely on the postselection of entanglement, which acts as an entanglement distillation operation. Improved generations of QRs may employ active error correction codes that necessitate much shorter link distances and a higher number of qubits (50–100, i.e. a quantum processor in the Sycamore scale) per node. Hence, we restrict our attention to the first generation type architectures that employ ensemble-based QMs. The use of atomic ensembles for long-distance communication was first proposed in a seminal paper by Duan, Lukin, Cirac and Zoller[34] also known as the DLCZ protocol. It relies on creating photon-spin wave entanglement through Raman scattering. This protocol has been modified and improved significantly over time[17,35,36]. Nevertheless, the entanglement distribution rate with these schemes quickly drops below practically useful levels above few thousand kilometres which renders reaching true global distances a formidable challenge with land-based architectures.

A hybrid, satellite-assisted architecture has been proposed for entanglement distribution with useful rates[37] (Fig. 1, top). It relies on satellites equipped with entangled photon pair sources communicating with the memory nodes located in ground stations. Other than the satellite links the main difference it exhibits with respect to other first-generation protocols is that heralding is performed via a quantum non-demolition (QND) measurement[38]. Entanglement is then distributed between the communicating parties via entanglement swapping operations between neighbouring nodes, similar to previous protocols. The authors cited technical challenges, such as launch and operation in the space environment, to favour placing QMs in ground stations. However, during the 6 years since the proposal, atomic physics experiments have made a leap into space, mainly for atom interferometry and optical clock applications. Thus the feasibility and performance of QR architectures that operate in space should be reexamined in light of these advancements (Fig. 1, bottom).

We consider a constellation with $2^{n+1}-1$ satellite, where n is the nesting level that divides the whole communication channel into 2^n segments. There are two types of satellites: one carries a photon pair source and the other carries QND and QM equipment for entanglement swapping (satellites with red stars and the dashed box in Fig. 1). Such a scheme will have several advantages over the original hybrid protocol. The first and most important is lower loss due to having only two atmospheric channels and the other internode links being located in space. The second advantage is that success will depend on the weather conditions only at two ground stations at the two ends of the communication link whereas the original proposal requires all ground stations (including intermediate relay stations) to simultaneously have good weather conditions, which becomes increasingly unlikely as the number of nodes increases (for a detailed treatment, see Supplementary Material). Finally, the need for Doppler-shift compensation to ensure indistinguishability of photons in a BSM is greatly reduced due to lower relative internode velocities.

As a figure of merit, we use total entanglement distribution time, T_{tot}, for the repeater calculations. The distributed entangled pairs then can be used for different applications such as QKD, distributed sensing or computation.

The time required to create and distribute an entangled state with the DLCZ protocol is given by[17]

$$T_{\mathrm{tot}}^{\mathrm{DLCZ}} = 3^{n+1}\frac{L_0}{c}\frac{\prod_{k=1}^{n}\left(2^k-\left(2^k-1\right)\eta_m\eta_d\right)}{\eta_d\eta_t p\left(\eta_m\eta_d\right)^{n+2}} \tag{1}$$

where we recall that n is the nesting level that divides the whole communication length L into 2^n links with L_0 length. η_d, η_t and η_m are detection efficiency, channel transmission and memory efficiency, respectively. We define $\eta_m = \eta_r\eta_w$ with η_r (η_w) being the memory read-out (write) efficiency. Lastly, p is the photon pair creation probability and c is the speed of light. Memories should be pumped to create a sufficient rate of photon pairs, i.e. high p but still low enough to minimise double pair emissions that scale as p^2. This assumes a single-mode memory and thus could be further reduced by using temporally multimode memories[39,40].

On the other hand, entanglement distribution time in the QND-QR protocol is given by[37]

$$T_{\mathrm{tot}}^{\mathrm{QND}} = \left[R_s\eta_s P_0^{\mathrm{avg}}\eta_{\mathrm{q}}^2\eta_{\mathrm{w}}^2\left(\frac{2}{3}\frac{\eta_{\mathrm{t}}^2\eta_{\mathrm{d}}^2}{2}\right)^n\right]^{-1}. \tag{2}$$

Here in addition to the parameters defined above, η_q is the QND detection efficiency, R_s is the source repetition rate and P_0^{avg} is the average two-photon transmission.

The main difference between calculations presented in this section and in the original hybrid satellite-ground architecture is

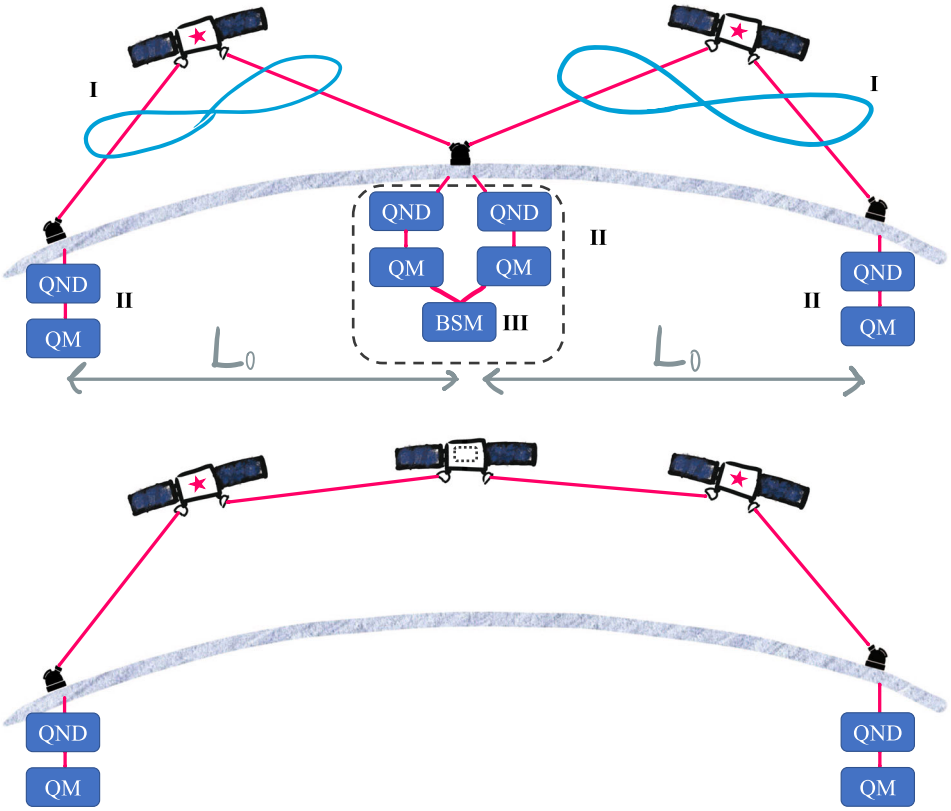

Fig. 1 Comparison of hybrid and fully space-based quantum repeater architectures. Top: Hybrid QND-QR protocol, following[37] with nesting level, $n = 1$ and segment length, L_0. Entangled photon pairs are created by on-board sources (red stars) and sent to ground stations (I). After a QND detection heralds the arrival of the photons they are loaded to QMs (II). BSM is performed between the memories to extend entanglement between end stations (III). Bottom: New architecture where the QND and QMs are also located on-board an orbiting satellite.

that only the two end links are satellite-ground links whereas all other optical channels are inter-satellite links. In Fig. 2 we present entanglement distribution times $T_{\text{tot}}^{\text{DLCZ}}$ and $T_{\text{tot}}^{\text{QND}}$. We assume a nesting level of $n = 3$ and an average fractional cloud coverage (fcc) of 0.54 in what follows.

Entanglement distribution time as a function of total ground distance is plotted in Fig. 2a. DLCZ protocols are significantly slower than the QND protocols. The main reason is the long waiting times for the classical heralding signal transmitted between neighbouring nodes. It is expressed with the factor L_0/c in Eq. (1) and accumulates as the distance, hence the loss, increases. Hybrid ground-space and full-space QND protocols start off within an order of magnitude but the scaling quickly turns against the hybrid protocol as atmospheric loss increases due to the increasingly narrow grazing angle and dominates the diffractive loss. The space-QND protocol offers three orders of magnitude faster entanglement generation rates for global distances.

The entanglement distribution time, T_{tot}, dictates the minimum required storage time, for the QM used in the repeater chain. If we look at Fig. 2a, the full space-based protocol proposed here requires a storage time of around 70 ms for 10^4 km ground distance and a 900 ms storage is required for a distance half the Earth's circumference. On the other hand, the hybrid protocol necessitates ~80 s and 50 mins for the same distances.

In Fig. 2b we plot T_{tot} as a function of beam divergence (e^{-2} beam divergence half-angle, Eq. (4)), $\Delta\theta$. Diffraction-limited beams at optical wavelengths has around 1 μrad divergence for telescope radii of around 20 cm. QND protocols are more sensitive to channel losses since they scale with η_t^{-2} whereas DLCZ schemes follow η_t^{-1} scaling. This sensitivity results in ~4 orders of magnitude slower operation times with an imperfect beam with 10 μrad divergence (similar to MICIUS) with respect to what can be achieved with a diffraction-limited beam. The scaling difference between DLCZ and QND protocols results in a hybrid-QND scheme having a comparable speed with the multimode DLCZ at large divergences. Although optical links (in the limit of large grazing angle) do not suffer from exponential losses such as in optical fibres, this example shows it is nevertheless crucial to have high quality beams with very small divergence.

Lastly, we investigate the effect of the finite memory efficiency on the entanglement distribution time in Fig. 2c. We again see that it is highly crucial to have highly efficient memories. For QND protocols, 50% memory efficiency reduces the operation speed by around six orders of magnitude when compared to 90% memory efficiencies for 2×10^4 km total link distance. Given that satellites only have few minutes of flyby over any target, this difference easily makes the whole protocol impractical.

So far we have concentrated on global scale quantum networking via satellite links. In what follows we analyse the MA-QKD proposals in a shorter range, line-of-sight setting.

MA-QKD schemes

As a more concrete example of using QMs in space, in this section, we adapt the well-established MA-QKD protocols to a space-based scenario. We benchmark the calculated key rates with MA-QKD protocols against a QKD protocol with entangled photons[41,42] (ent-QKD) that does not rely on the violation of Bell's inequality. In

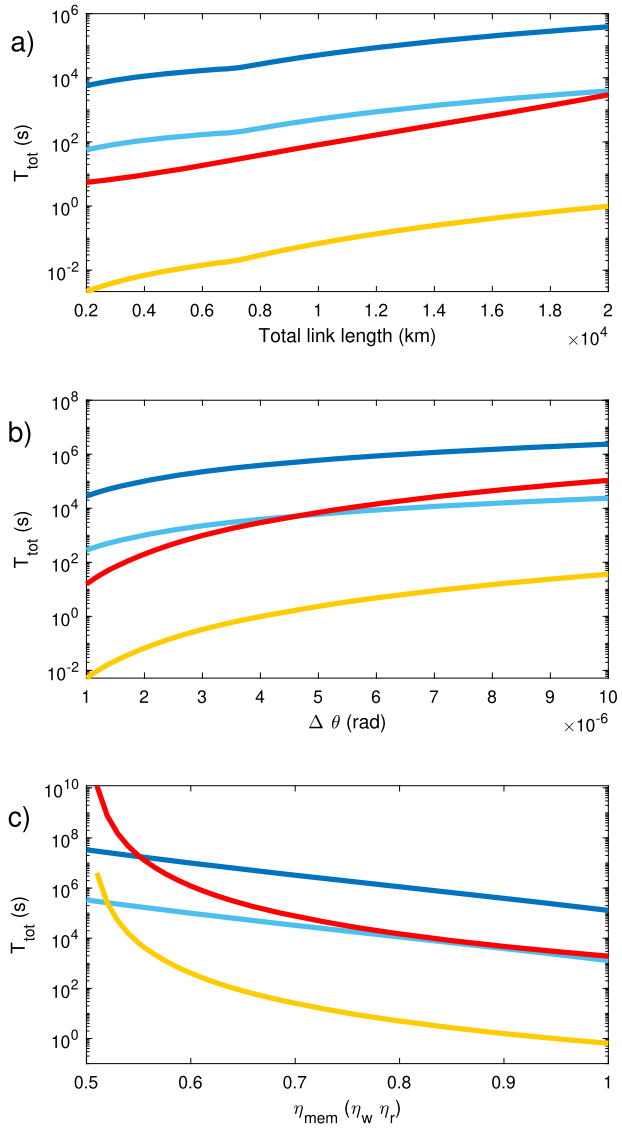

Fig. 2 Time to distribute an entangled pair as a function of different parameters. a total distance, **b** beam divergence and **c** memory efficiency. Within each plot: DLCZ with single (dark blue) or 100 mode (light blue) memory, hybrid-QND (red) and space-QND protocols (orange). The nominal assumed parameters (when not varied) are nonideal Gaussian beams with divergence $\Delta\theta = 4$ μrad, $L = 20{,}000$ km and $\eta_r\eta_w \equiv \eta_{mem} = 0.9$, with $\eta_r = \eta_w$. We fix $\eta_q = 0.9$, $\eta_s = 1$, $R_s = 20$ MHz and an average fcc = 0.54.

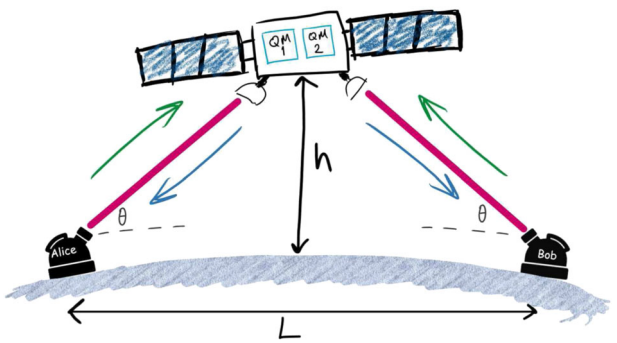

Fig. 3 MA-QKD protocol, following[32,33], in the geometry of[23,75]. Green (blue) arrows show the uplink (downlink) protocol. Alice and Bob both have standard BB84 encoders. QM quantum memory, θ elevation, h orbital height, L total ground communication distance.

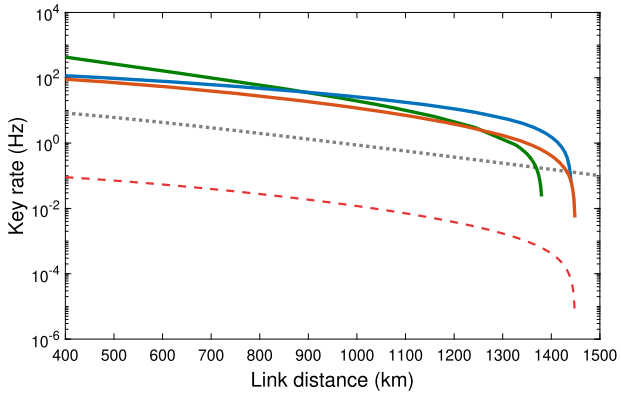

Fig. 4 Comparison of MA-QKD schemes with ent-QKD (no memory) protocol. Grey dotted: ent-QKD ($R_s = 20$ MHz); blue: uplink configuration with storage time 5 ms; solid (dotted) red: downlink configuration, with $N = 1000$ (single) temporal modes with storage time 7.5 s; green: downlink with $N = 1000$ temporal modes and $m = 100$ memory pairs with storage time 100 ms.

Fig. 3, we consider different configurations, i.e. both uplink and downlink.

Figure 4 shows the achievable key rate as a function of ground distance L with (i) ent-QKD protocol, i.e. no QM (grey dashed)[42]; (ii) uplink configuration with protocol presented in ref. [31,32] (blue) and finally (iii) downlink scenario with a single memory pair ($m = 1$, red) and 100 memory pairs ($m = 100$, green)[43]. Parameters used in simulations to generate Figs. 4 and 5 are shown in Table 1.

The model presented here predicts a secret key rate of 0.15 bits/s at 1120 km ground distance with a 5.9 MHz repetition rate without memories and this value is consistent with the recently reported value of 0.12 bits/s by the MICIUS team[23]. For the simulations discussed here, we assume a repetition rate of 20 MHz that yields around 1 bit/s at 1000 km ground distance. We will use this value to benchmark the performance of MA-QKD schemes.

Uplink: The protocol proposed in refs. [31,32] relies on communicating parties on the ground using single-photon sources with conventional BB84 encoders and sending them up to a satellite that acts as a middle station where they would each be stored in an individual QM. Memories will then be read out upon the successful heralded loading of both. A BSM is then performed on the retrieved photons to extract a key or perform entanglement swapping (Fig. 1). One of the key characteristics of this protocol is its high operating rate as there is no waiting time associated with the heralding signal travelling between the BSM station and the communicating parties. However, this geometry precludes the extension of this protocol into a repeater architecture. A central requirement of this scheme is the heralding of a successful memory loading process. Ref. [32] analyses both direct and indirect heralding scenarios. The directly heralded scheme relies on the QND detection of incoming photons before being loaded into their respective QMs whereas the indirectly heralded scheme requires additional BSMs that herald the entanglement between the individual memories and the respective incoming photons. A BSM between the memories is then performed to distil a secret key.

The main drawback of the uplink geometry is the additional loss contribution due to the atmospheric diffraction happening early in the optical path[22,44], also called the shower-curtain effect. This additional loss varies strongly with the specific weather conditions and can be as big as 20 dB compared with downlink transmission. Thus bigger receiver apertures in space are required which might be challenging to deploy.

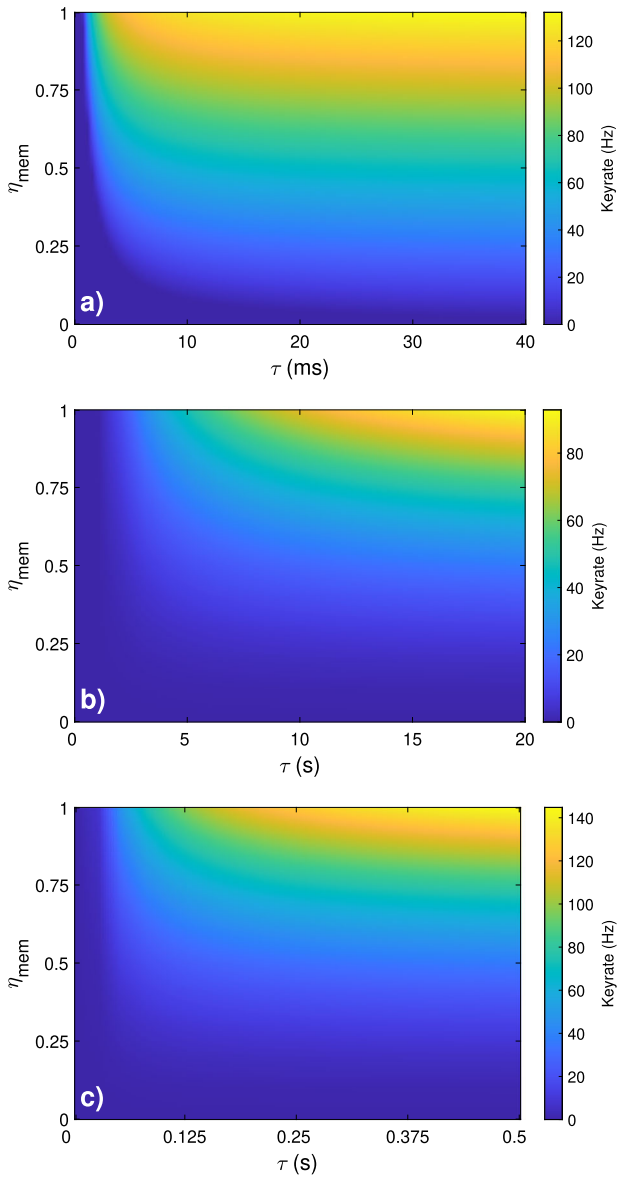

Fig. 5 Achievable key rates at 1000 km ground distance. a Uplink configuration with $m = 1$. **b** Downlink configuration with $m = 1$, $N = 1000$. **c** Downlink configuration with $m = 100$, $N = 1000$.

Table 1. Parameters used in MA-QKD simulations.

Description	Parameter	Downlink	Uplink
Orbital height	h	400 km	400 km
Sender aperture radii	R_{sender}	15 cm	15 cm
Receiver aperture radii	R_{receiver}	50 cm	50 cm
Divergence	$\Delta\theta$	10 μrad	10 μrad
Storage time	τ	100 ms, 7.5 s	25 ms
Memory pairs	m	100, 1	1
Memory efficiency	η_{mem}	0.8	0.8
Detector efficiency	η_{det}	0.7	0.7

The blue curve in Fig. 4 shows the expected key rate obtained with the protocol in ref. [32]. We assume 15 cm (50 cm) of radius for the sender (receiver) telescope, with 10 μrad beam divergence and we omitted atmospheric turbulence and the shower-curtain effect. The memory is assumed to perform with a storage time of 5 ms and 80% combined write-read efficiency. The operation rate is assumed to be 20 MHz and we only consider single-mode memory case as the operation rate is not limited to any classical communication between parties. As can be seen, this protocol offers a speedup over the no-memory protocol up to ~1450 km after which no key could be generated.

Figure 4 shows the achievable key rate at a fixed $L_0 = 1000$ km as a function of memory write efficiency and storage time. It is observed that no meaningful key rate could be achieved with memory dephasing times of <5 ms, regardless of the memory efficiency. The dependence on memory efficiency is less dramatic for the uplink protocol. With a relatively modest storage time of 20 ms and memory write efficiency of around 50%, one can achieve more than an order of magnitude improvement over the no-memory case as summarised above. However, one should note that this architecture can not be extended to a quantum repeater architecture due to the photon travel direction precluding any entanglement swapping operation between neighbouring links.

Downlink: The other main MA-QKD protocol we analyze was first proposed in 2014[33]. Here the direction of travel of the photons is from the middle station to the communicating stations at the two ends. In this configuration, each of the QMs in the middle station emits single photons that are entangled with the internal states of the respective memories towards the receiving ends. A BSM will be performed on the memories upon the successful BB84 measurements by the receiving parties. The repetition rate of the protocol is inherently limited by the speed of light travel time of classical signals to herald a successful detection by the communicating parties to the middle station where the BSM is performed. This also requires long-lived QMs with storage times in the order of seconds to achieve similar performance to the previous method. An extension of this protocol in which the central pair of QMs are replaced with m pairs of QMs[43] reduces the required storage time.

The operation rate of the downlink protocol is intrinsically limited (for a single-mode memory) by the time the classical signal takes to reach the other party, i.e. $R = c/2L_{\text{LoS}}$, with c being the speed of light and L_{LoS} is the line-of-sight distance between a ground station and the satellite. Hence, this protocol requires long storage times, in the order of seconds. In Fig. 4 the dotted red curve shows the key rate with a single-mode QM. The achievable key rate is significantly lower than protocol due to the slower operation speed. The only way to increase the key rate is thus to operate with temporally multimode QMs. The solid red curve shows the key rate that is only possible with a QM that could store 1000 temporal modes. This provides an enhancement of around an order of magnitude between line-of-sight distances of 500–1000 km. Figure 5b shows the achievable key rate as a function of the memory efficiency and dephasing time at a fixed ground distance of 1000 km, with $N = 1000$ temporal mode QM. At such a distance storage times shorter than 5 s would not be sufficient for the protocol to produce any meaningful key rate regardless of the storage efficiency. Likewise, storage efficiency of around 35% is needed in combination with a $\tau = 10$ s to reach a 10 Hz key rate.

We further analysed the extension of this protocol with $m = 100$ pairs of QMs located in the middle station. The green curve in Fig. 4 shows that a storage time of only 100 ms is sufficient instead of the very demanding 7.5 s to reach the same distance with similar key rates. Figure 5c shows the performance map of this scheme again at a fixed ground distance of 1000 km. The striking feature here is that the cut-off storage time below which no key could be transmitted in only a few ms.

One can also use brighter photon-pair sources to increase the achievable key rates by increasing R_S[45]. With the deployment of such fast sources, GHz-bandwidth QMs[46] would be still useful to further increase the achieved key rates.

Candidate memory platforms

In this section, we overview the existing QM experiments and provide a roadmap towards choosing a proper physical system in light of the findings of the previous section. We focus on ensemble-based systems as it would be more straightforward to implement temporally multimode storage needed in the protocols described in this paper. However, we note that the first land-based MA-QKD experiment has been recently performed with a single colour centre in diamond at mK temperatures[47].

Warm vapour memories. Photon storage in the long-lived ground states of alkaline vapours at room temperature is particularly appealing, as it requires neither complex cooling mechanisms nor large magnetic fields. This makes such memories ideal for field applications in remote environments, e.g. undersea or in space. The performance of warm vapour memories has been continuously improved since the first demonstrations of memories based on electromagnetically induced transparency (EIT) in the 2000s. In recent years, the development of QM implementations in alkaline vapour have gained remarkable momentum: (i) A vapour cell memory reached a storage time of $\tau = 1$ s by using spin-orientation degrees of freedom and anti-relaxation coatings[48]. (ii) The efficiency of a room temperature EIT-like memory was pushed beyond 80%[46]. (iii) EIT-like QMs with ~1 GHz bandwidths were developed[49]. These could in principle be extended to the storage of multiple signals in individually addressable subcells, as realised in cold atomic ensembles[50].

Besides ground state EIT memory, another promising vapour cell memory concept is the storage of photonic quantum information in highly excited atomic orbitals. These orbitals are relatively long-lived, allowing for storage times on the order of 100 ns. The fast ladder memory scheme is based on two-photon off-resonant cascaded absorption[51,52]. This scheme allows for virtually noise-free storage with acceptance bandwidths in the GHz regime, but it needs to be further developed to allow for the comparable long storage times required by long-distance quantum communications.

Laser-cooled atomic systems. These are well-established platforms for quantum information storage. High efficiency[53], temporal[40] and spatial multimode storage[50] have been performed among many other experiments in the last years. There has been a growing interest in deploying cold-atom experiments in space for more than a decade. This is driven by a combination of a desire for access to longer periods of microgravity for fundamental research, and the deployment of instruments such as optical clocks on satellites for future global positioning concepts. Cold atom ensembles and Bose–Einstein condensates have already been created on orbiting platforms including Tiangong-2[54] and the ISS[55,56].

Cold atom experiment on board ISS. In the context of these platforms, BECCAL is of particular interest due to the variety of experiments it is designed to perform. These experiments include the possibility of conducting initial demonstrations of QMs in space. In short, BECCAL[57] will be capable of producing 3D-MOTs of 2×10^9 ^{87}Rb atoms, 10^9 ^{85}Rb atoms, 8×10^8 ^{39}K atoms, 4×10^8 ^{41}K atoms and 10^7 ^{40}K atoms in single species operation, it will also be possible to obtain single species BECs of 10^6 ^{87}Rb atoms, or 10^5 ^{41}K atoms. Atoms can also be confined in a 1064 nm dipole trap with a waist of 100 µm and a tunable potential depth of 0.01 to 5 µK. Quantum coherences of longer than 5 s are planned. Due to the absence of gravity, atomic samples can be used without additional, gravity compensating, trapping potentials. Within BECCAL, the possibility for QM experiments is mediated via the detection scheme. Absorption detection is performed via two perpendicular axes to allow the gathering of three-dimensional information about atom clouds. Via a distribution and switching system, it is possible to deliver light addressing the D2-lines of rubidium and potassium in a variety of pulse schemes (the $5^2S_{1/2} \rightarrow 5^2P_{3/2}$ and $4^2S_{1/2} \rightarrow 4^2P_{3/2}$ transitions in Rb and K, respectively). One can deliver 'cooling' and 'repump' frequencies (i.e. $F = 2 \rightarrow F' = 3$ and $F = 1 \rightarrow F' = 2$, respectively for ^{87}Rb) simultaneously or consecutively on a single axis, or in a crossed beam arrangement with cooling on one axis and repump on the other. Each frequency can be switched independently in less than 1 µs. These flexible conditions will facilitate storage techniques such as EIT in a microgravity environment thus being a pathfinder and demonstrator for the technology discussed in this paper.

Rare-earth ion-doped crystals (REIDs). These are another major platform to realise QMs in the context of quantum communication. Some of the recent advances include but are not limited to; demonstration of quantum correlations between long-lived hyperfine states and telecom photons[58], demonstrating 6-h coherence time[59] and hour-long bright pulse storage[60]. The other research front in REID field is the miniaturisation of these experiments. Waveguide geometries[61,62] offer enhanced compactness. The storage bandwidth is usually limited to a few MHz due to narrow hyperfine level separation however recent electronic-nuclear hybrid storage protocols would open up possibilities of storing large bandwidth photons in the long-lived spin states[63], this would enable higher operation rates, R_s. A combination of compactness, high-bandwidth storage capability together with high efficiency and long storage times would place REID systems at the forefront of QM systems for space applications. On top of material considerations, REIDs are also suitable for temporally multimode storage[39,64,65]. REIDs could be a promising candidate to realise a space-based QR with the development of miniature, space-compatible cryostats[66].

DISCUSSIONS

Quantum cryptography is the framework behind novel entanglement distribution protocols and security proofs. It has rapidly developed from simple lab demonstrations to in-field applications. However, developing and implementing robust QKD protocols over global transmission lengths remains an open challenge. The use of both ground and satellite-based quantum repeater networks provide the most promising solution to extend quantum communications to global scales.

In this work, we provide one of the first theoretical analysis towards this goal. Our study provides a more complete investigation of the use of QMs on key rates for concrete line-of-sight distance QKD protocols. We also analyse the effect of different experimental parameters such as beam divergence and memory efficiency on the performance of these protocols. Our proposal uses satellites equipped with QMs in LEO that implement MA-QKD. We benchmark entanglement distribution times achieved through our architecture with existing protocols to find an improvement of ~3 orders of magnitude over global scales. With the majority of optical links now in space, a major strength of our scheme is its increased robustness against atmospheric losses. We further demonstrate that QMs can enhance secret key rates in general line-of-sight QKD protocols. Generally, significant memory performance improvements are required. These include highly multimode storage in combination with a long lifetime and highly efficient operation. Our work thus provides a practical roadmap towards the implementation of QMs for space-based fundamental physics experiments[67] and opens up the way to a promising realisation of a truly global untrusted quantum network. Recent, complementary work also looked at space-QR schemes with a particular focus on the optimisation of the nesting levels for a given distance and included a cost analysis of deployment and operation of such architectures[68].

Our work leads to further interesting research questions. It would be interesting to explore the effects of orbital dynamics and constellation designs on entanglement distribution times. This naturally leads to the question of engineering efficient satellite network topologies, where QMs with even modest coherence times can effect profound gains to entanglement rates[69]. Moreover, it would be interesting to explore the practical effects of finite block sizes on the key rate[70], for example, effects owing to a transmission time window between satellites and ground stations.

METHODS

Quantum link modelling and channel losses

An important requirement for the estimation of the performance of a space-based quantum communication system is the precise modelling of the optical loss and source of noise of the channel as they both decrease the secret key rate. The former by making the transmitted quantum states less distinguishable by the receiver, and thus decreasing the overall detection rate, and the latter by increasing the Quantum Bit Error Rate (QBER).

Diffraction losses. The dominant source of loss is diffraction which for a Gaussian mode of initial beam waist ω_0 and wavelength λ travelling a distance d is given by[71]:

$$\eta_{\mathrm{dif}} = 1 - \exp\left[-\frac{D_R^2}{2\omega_d^2}\right] \quad \text{with} \quad \omega_d^2 = \omega_0^2\left[1 + \left(\frac{\lambda d}{\pi\omega_0^2}\right)^2\right] \tag{3}$$

Where ω_d is the accumulated beam waist at distance d from the source and D_R is the receiver aperture. As one can see, diffraction losses can be mitigated by increasing the receiver aperture but this could be unfeasible due to payload constraints. However, one should note that diffraction losses scales quadratically with the link distance (for $d \gg \pi\omega_0^2/\lambda$) contrary to the exponential scaling for a fibre link with the length of the fibre. The divergence $\Delta\theta$ of an imperfect Gaussian beam is characterised by its M^2 value through the following relation:

$$\Delta\theta = M^2\frac{\lambda}{\pi\omega_0}. \tag{4}$$

Atmospheric losses. Atmosphere constituents cause absorption and scattering of the optical signal, those effects depend on the signal

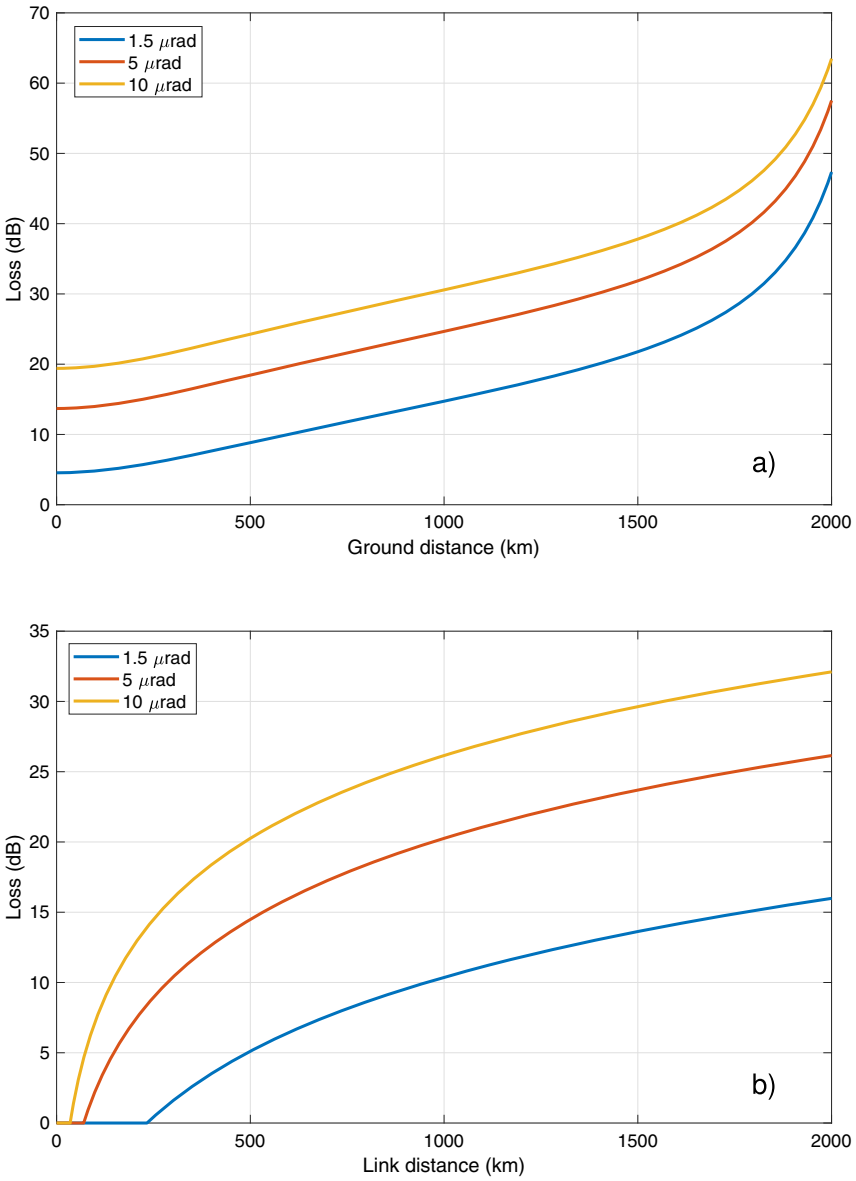

Fig. 6 Optical channel losses with different beam divergences. a Satellite-ground connection. **b** Satellite-satellite connection. Blue: 1.5 μrad, red: 5 μrad and yellow: 10 μrad beam divergence, respectively.

Table 2. Wavelengths (λ) and $\eta_{\text{atm}}^{\pi/2}$ for several quantum memory platforms.

Atomic system	Transition	λ (nm)	$\eta_{\text{atm}}^{\pi/2}$
Eu^{3+}: Y_2SiO_5	$^7F_0 \rightarrow {}^5D_0$	580	0.65
Pr^{3+}: Y_2SiO_5	$^3H_4 \rightarrow {}^1D_2$	606	0.67
^{87}Rb	$5^2S_{1/2} \rightarrow 5^2P_{3/2}$	780	0.79
^{87}Rb	$5^2S_{1/2} \rightarrow 5^2P_{1/2}$	795	0.77
^{133}Cs	$6^2S_{1/2} \rightarrow 6^2P_{3/2}$	852	0.81
^{133}Cs	$6^2S_{1/2} \rightarrow 6^2P_{1/2}$	894	0.64

wavelength. The atmospheric loss that includes absorption as a function of elevation angle of θ is given by[28]:

$$\eta_{\text{atm}}(\theta) = \left(\eta_{\text{atm}}^{\pi/2}\right)^{\csc\theta} \tag{5}$$

Here $\eta_{\text{atm}}^{\pi/2}$ is the transmissivity at Zenith and can be computed from a given model for the atmospheric absorption $\gamma(r;\lambda)$ as:

$$\eta_{\text{atm}}^{\pi/2} = \int_0^h dr\ \gamma(r;\lambda) \tag{6}$$

where h is the altitude of the satellite. The value of $\eta_{\text{atm}}^{\pi/2}$ can also being found using dedicated software such as MODTRAN[72], at 780 nm ($^{87}RbD_2$ line, $5^2S_{1/2} \rightarrow 5^2P_{3/2}$ transition) the Zenith transmissivity is about 80% (in Table 2 we list values for several other QM platforms).

Pointing losses. Vibration and mechanical stress due, for example to thermal dilation, cause an error in the point and further loss. By assuming that the distribution for pointing error angle follows is a Gaussian with zero mean and σ_{point} standard deviation, this loss contribution can be modelled as[73]:

$$\eta_{\text{point}} = \exp\left[-8\sigma_{\text{point}}^2/\omega_0^2\right], \tag{7}$$

for a diffraction-limited beam at optical wavelength, a point error of 1 μrad causes a decrease of the transmittance of about 10%. Figure 6 shows the channel losses when we only consider the diffractive losses and atmospheric absorption. Beam tracking errors are not included. We assume a transmitting (receiver) telescope radius of 0.15 m (0.5 m) and a low-earth orbit with $h = 400$ km. Figure 6a shows that atmospheric loss becomes dominant at large distances with decreasing grazing angle. Figure 6b shows inter-satellite losses where only diffractive losses are considered.

Dark counts. For a Silicon-based APD the dark count rate is estimated to be around 10 counts/s, such value could be improved by several orders of magnitude by using SNSPDs. In this article, we assumed $p_d = 10^{-6}$ for a ~1 μs detection window which corresponds to a few Hz dark count rate.

Stray light. The sources of stray light are divided into natural sources, such as the moon and the stars, and the artificial one, the so-called sky glow, produced by the diffusion of light from human activities. Stray light can be decreased by spectral and time filtering. The number of stray counts in an acquisition window is given by[74]:

$$N = \frac{\lambda}{hc} H_{\text{sky}} \Omega_{\text{FoV}} \left(\frac{\pi D_R}{2}\right)^2 \Delta\lambda \Delta t, \tag{8}$$

where H_{sky} is the total sky brightness and $\Delta\lambda$ is the spectral bandwidth and Δt is the detection window. It is worth noting that, in the optical domain, the number of stray photons can vary by several orders of magnitude according to the sky condition, e.g. the presence of the Moon[74].

Key rate calculations

For numerical calculations of the secret key rate, we consider a pair of QMs that send entangled photons to their respective end users as illustrated in Fig. 1. The performance of this MA protocol is assessed in terms of the secret key rate achievable by the BB84 cryptographic protocol. The secret key rate for this is lower bounded by refs. [32,33]

$$R = \frac{Y}{2}[1 - h(e_X) - fh(e_Z)], \tag{9}$$

where Y is the probability per channel use that both Alice and Bob's measurements and the Bell state measurement was successful, e_X (e_Z) is the QBER in the X (Z) basis, f is the error correction inefficiency and $h(e)$ is the binary entropy function defined via $h(e) = -e\log_2 e - (1-e)\log_2(1-e)$. Details of how Y and the individual errors are calculated can be found in refs. [32,42,43].

DATA AVAILABILITY

The data generated during this work are available from the corresponding author M. G. upon reasonable request.

CODE AVAILABILITY

The code used for generating the plots are available from the corresponding author M.G. upon reasonable request.

Received: 22 June 2020; Accepted: 14 July 2021;
Published online: 18 August 2021

REFERENCES

1. Deutsch, D. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. R. Soc. A* **400**, 97 (1985).
2. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th Symposium on Foundations of Computer Science* 124–134 (IEEE Computer Society, 1994).
3. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
4. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
5. Degen, C. L., Reinhard, F. & Cappellaro, P. Quantum sensing. *Rev. Mod. Phys.* **89**, 035002 (2017).
6. Sidhu, J. S. & Kok, P. Geometric perspective on quantum parameter estimation. *AVS Quantum Sci.* **2**, 014701 (2020).
7. Sidhu, J. S., Ouyang, Y., Campbell, E. T. & Kok, P. Tight bounds on the simultaneous estimation of incompatible parameters. *Phys. Rev. X* **11**, 011028 (2021a).
8. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595 (2014).
9. G. Mélen, G. et al. Handheld quantum key distribution. In *2018 Conference on Lasers and Electro-Optics* (*CLEO*) 1–2 (OSA, 2018).
10. Sibson, P. et al. Chip-based quantum key distribution. *Nat. Commun.* **8**, 13984 (2017).
11. Boaron, A. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
12. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **92**, 025002 (2020).
13. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photon.* **12**, 1012 (2020).
14. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400 (2018).
15. Chen, J.-P. et al. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).
16. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802 (1982).
17. Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33 (2011).
18. Muralidharan, S. et al. Optimal architectures for long distance quantum communication. *Sci. Rep.* **6**, 20463 (2016).
19. Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys.* **2**, 51 (2019).
20. Vinay, S. E. & Kok, P. Practical repeaters for ultralong-distance quantum communication. *Phys. Rev. A* **95**, 052336 (2017).
21. Sit, A. et al. High-dimensional intracity quantum cryptography with structured photons. *Optica* **4**, 1006 (2017).
22. Bedington, R., Arrazola, J. M. & Ling, A. Progress in satellite quantum key distribution. *npj Quantum Inf.* **3**, 30 (2017).

23. Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **582**, 501 (2020).
24. Sidhu, J. S., Brougham, T., McArthur, D., Pousa, R. G. & Oi, D. K. L. Finite key effects in satellite quantum key distribution. Preprint at arXiv 2012.07829 (2020).
25. Sidhu, J.S., et al. Advances in space quantum communications. *IET Quant. Comm.* 1–36 (2021). https://doi.org/10.1049/qtc2.12015.
26. Liao, S.-K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 030501 (2018).
27. Oi, D. K. et al. Cubesat quantum communications mission. *EPJ Quantum Technol.* **4**, 6 (2017).
28. Khatri, S., Brady, A. J., Desporte, R. A., Bart, M. P. & Dowling, J. P. Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet. *npj Quantum Inf.* **7**, 4 (2021).
29. Vergoossen, T., Loarte, S., Bedington, R., Kuiper, H. & Ling, A. Modelling of satellite constellations for trusted node qkd networks. *Acta Astronaut.* **173**, 164 (2020).
30. Mazzarella, L. et al. Quarc: quantum research cubesat -a constellation for quantum communication. *Cryptography* **4**, 7 (2020).
31. Abruzzo, S., Kampermann, H. & Bruß, D. Measurement-device-independent quantum key distribution with quantum memories. *Phys. Rev. A* **89**, 012301 (2014).
32. Panayi, C., Razavi, M., Ma, X. & Lütkenhaus, N. Memory-assisted measurement-device-independent quantum key distribution. *N. J. Phys.* **16**, 043005 (2014).
33. Luong, D., Jiang, L., Kim, J. & Lütkenhaus, N. Overcoming lossy channel bounds using a single quantum repeater node. *Appl. Phys. B* **122**, 96 (2016).
34. Duan, L.-M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413 (2001).
35. Sangouard, N. et al. Long-distance entanglement distribution with single-photon sources. *Phys. Rev. A* **76**, 050301 (2007).
36. Chen, Z.-B., Zhao, B., Chen, Y.-A., Schmiedmayer, J. & Pan, J.-W. Fault-tolerant quantum repeater with atomic ensembles and linear optics. *Phys. Rev. A* **76**, 022329 (2007).
37. Boone, K. et al. Entanglement over global distances via quantum repeaters with satellite links. *Phys. Rev. A* **91**, 052325 (2015).
38. Rispe, A., He, B. & Simon, C. Photon-photon gates in Bose-Einstein condensates. *Phys. Rev. Lett.* **107**, 043601 (2011).
39. Kutluer, K., Mazzera, M. & de Riedmatten, H. Solid-state source of nonclassical photon pairs with embedded multimode quantum memory. *Phys. Rev. Lett.* **118**, 210502 (2017).
40. Heller, L., Farrera, P., Heinze, G. & de Riedmatten, H. Cold-atom temporally multiplexed quantum memory with cavity-enhanced noise suppression. *Phys. Rev. Lett.* **124**, 210504 (2020).
41. Jennewein, T., Simon, C., Weihs, G., Weinfurter, H. & Zeilinger, A. Quantum cryptography with entangled photons. *Phys. Rev. Lett.* **84**, 4729 (2000).
42. Ma, X., Fung, C.-H. F. & Lo, H.-K. Quantum key distribution with entangled photon sources. *Phys. Rev. A* **76**, 012307 (2007).
43. Trényi, R. & Lütkenhaus, N. Beating direct transmission bounds for quantum key distribution with a multiple quantum memory station. *Phys. Rev. A* **101**, 012325 (2020).
44. Bourgoin, J.-P. et al. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *N. J. Phys.* **15**, 023006 (2013).
45. Lohrmann, A., Perumangatt, C., Villar, A. & Ling, A. Broadband pumped polarization entangled photon-pair source in a linear beam displacement interferometer. *Appl. Phys. Lett.* **116**, 021101 (2020).
46. Guo, J. et al. High-performance raman quantum memory with optimal control in room temperature atoms. *Nat. Commun.* **10**, 148 (2019).
47. Bhaskar, M. K. et al. Experimental demonstration of memory-enhanced quantum communication. *Nature* **580**, 60 (2020).
48. Katz, O. & Firstenberg, O. Light storage for one second in room-temperature alkali vapor. *Nat. Commun.* **9**, 2074 (2018).
49. Wolters, J. et al. Simple atomic quantum memory suitable for semiconductor quantum dot single photons. *Phys. Rev. Lett.* **119**, 060502 (2017).
50. Pu, Y.-F. et al. Experimental realization of a multiplexed quantum memory with 225 individually accessible memory cells. *Nat. Commun.* **8**, 15359 (2017).
51. Kaczmarek, K. T. et al. High-speed noise-free optical quantum memory. *Phys. Rev. A* **97**, 042316 (2018).
52. Finkelstein, R., Poem, E., Michel, O., Lahad, O. & Firstenberg, O. Fast, noise-free memory for photon synchronization at room temperature. *Sci. Adv.* **4**, eaap8598 (2018).
53. Bao, X.-H. et al. Efficient and long-lived quantum memory with cold atoms inside a ring cavity. *Nat. Phys.* **8**, 517 (2012).
54. Liu, L. et al. In-orbit operation of an atomic clock based on laser-cooled 87rb atoms. *Nat. Commun.* **9**, 2760 (2018).
55. Elliott, E. R., Krutzik, M. C., Williams, J. R., Thompson, R. J. & Aveline, D. C. Nasaas cold atom lab (cal): system development and ground test status. *npj Microgravity* **4**, 16 (2018).
56. Aveline, D. C. et al. Observation of bose-einstein condensates in an earth-orbiting research lab. *Nature* **582**, 193 (2020).
57. Frye, K. et al. The bose-einstein condensate and cold atom laboratory. *EPJ Quantum Technol.* **8**, 1 (2021).
58. Seri, A. et al. Quantum correlations between single telecom photons and a multimode on-demand solid-state quantum memory. *Phys. Rev. X* **7**, 021028 (2017).
59. Zhong, M. et al. Optically addressable nuclear spins in a solid with a six-hour coherence time. *Nature* **517**, 177 (2015).
60. Ma, Y., Ma, Y.-Z., Zhou, Z.-Q., Li, C.-F. & Guo, G.-C. One-hour coherent optical storage in an atomic frequency comb memory. *Nat. Commun.* **12**, 2381 (2021).
61. Marzban, S., Bartholomew, J. G., Madden, S., Vu, K. & Sellars, M. J. Observation of photon echoes from evanescently coupled rare-earth ions in a planar waveguide. *Phys. Rev. Lett.* **115**, 013601 (2015).
62. Corrielli, G., Seri, A., Mazzera, M., Osellame, R. & de Riedmatten, H. Integrated optical memory based on laser-written waveguides. *Phys. Rev. Appl.* **5**, 054013 (2016).
63. Businger, M. et al. Optical spin-wave storage in a solid-state hybridized electron-nuclear spin ensemble. *Phys. Rev. Lett.* **124**, 053606 (2020).
64. Gündoğan, M., Ledingham, P. M., Kutluer, K., Mazzera, M. & de Riedmatten, H. Solid state spin-wave quantum memory for time-bin qubits. *Phys. Rev. Lett.* **114**, 230501 (2015).
65. Jobez, P. et al. Towards highly multimode optical quantum memory for quantum repeaters. *Phys. Rev. A* **93**, 032327 (2016).
66. You, L. et al. Superconducting nanowire single photon detection system for space applications. *Opt. Express* **26**, 2965 (2018).
67. Rideout, D. et al. Fundamental quantum optics experiments conceivable with satellites—reaching relativistic distances and velocities. *Classical Quantum Gravity* **29**, 224011 (2012).
68. Liorni, C., Kampermann, H. & Bruß, D. Quantum repeaters in space. *N. J. Phys.* **23**, 053021 (2021).
69. Pant, M. et al. Routing entanglement in the quantum internet. *npj Quantum Inf.* **5**, 25 (2019).
70. Lorenzo, G. C. & Razavi, M. Finite-key analysis for memory-assisted decoy-state quantum key distribution. *N. J. Phys.* **22**, 103005 (2020).
71. Gagliardi, R. M. & Karp, S. *Optical Communications* 2nd edn (Wiley, 1995)
72. Berk, A. et al. In *Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery XX* Vol. 9088, (eds Velez-Reyes, M & Kruse, F. A) (SPIE, 2014).
73. Kaushal, H. & Kaddoum, G. Free space optical communication: challenges and mitigation techniques. Preprint at https://arxiv.org/abs/1506.04836 (2015).
74. Marshall, W. K. & Burk, B.D. In *The Telecommunications and Data Acquisition Report* (ed Posner, E. C.) (NASA, Jet Propulsion Laboratory 1986).
75. Yin, J. et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**, 1140 (2017).

ACKNOWLEDGEMENTS

M.G. and M.K. acknowledge the support by the German Space Agency DLR with funds provided by the Federal Ministry of Economics and Technology (BMWi) under grant numbers 50WM1958 (OPTIMO), 50WM2055 (OPTIMO-2), which made this work possible. M.G. further acknowledges funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 894590. V.H. acknowledge the support by the German Space Agency DLR with funds provided by the Federal Ministry of Economics and Technology (BMWi) under grant number 50WP1702 (BECCAL). D.K.L.O. is supported by the EPSRC Researcher in Residence programme (EP/T517288/1). J.S.S., L.M. and D.K.L.O. acknowledge the travel support by the EU COST action QTSpace (CA15220), and L. M. acknowledges the travel support by Scottish Universities Physics Alliance SUPA (LC17683). Funding was provided by the UK Space Agency through the National Space Technology Programme (NSTP3-FT-063 "Quantum Research CubeSat", NSTP Fast Track "System Integration & Testing of a CubeSat WCP QKD Payload to TRL5"), EPSRC Quantum Technology Hub in Quantum Communication Partnership Resource (EP/M013472/1) and Phase 2 (EP/T001011/1), and Innovate UK (EP/S000364/1). M.G. acknowledges Guillermo Currás Lorenzo for double-checking the code for MA-QKD calculations and pointing to few minor errors at an early stage of the work and Mohsen Razavi and Julius Wallnöfer for stimulating discussions.

AUTHOR CONTRIBUTIONS

M.G., J.W., D.K.L.O. and M.K. conceived this project. M.G. and J.S.S. designed the study and M.G. performed the calculations with inputs and feedback from all authors. M.G. and J.S.S. wrote the manuscript with contributions from all authors. M.K. supervised the project.

FUNDING

Open Access funding enabled and organized by Projekt DEAL.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-021-00460-9.

Correspondence and requests for materials should be addressed to M.Ga.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.