Research Article

OPTICA QUANTUM

Time-delayed single satellite quantum repeater node for global quantum communications

Mustafa Gündoğan,[1,*] Jasminder S. Sidhu,[2] Markus Krutzik,[1,3] and Daniel K. L. Oi[2,4]

[1]Institut für Physik and IRIS Adlershof Humboldt-Universität zu Berlin, Newtonstr. 15, Berlin 12489, Germany
[2]SUPA Department of Physics, University of Strathclyde, John Anderson Building, 107 Rottenrow East, Glasgow, G4 0NG, UK
[3]Ferdinand-Braun-Institut (FBH), Gustav-Kirchoff-Str. 4, Berlin 12489, Germany
[4]Walton Institute for Information and Communication Systems Science, South East Technological University, Waterford, X91 P20H, Ireland
*mustafa.guendogan@physik.hu-berlin.de

Received 5 January 2024; revised 29 February 2024; accepted 6 April 2024; published 1 May 2024

Global-scale quantum networking faces significant technical and scientific obstacles. Quantum repeaters (QRs) have been proposed to overcome the inherent direct transmission range limit through optical fiber. However, QRs are typically limited to a total distance of a few thousand kilometers and/or require extensive hardware overhead. Recent proposals suggest that strings of space-borne QRs with on-board quantum memories (QMs) are able to provide global coverage. Here, we propose an alternative to such repeater constellations using a single satellite with two QMs that effectively acts as a time-delayed version of a single QR node. By physically transporting stored qubits, our protocol improves long-distance entanglement distribution with reduced system complexity over previous proposals. We estimate the amount of secure key in the finite block regime and demonstrate an improvement of at least three orders of magnitude over prior single-satellite methods that rely on a single QM, while simultaneously reducing the necessary memory capacity similarly. We propose an experimental platform to realize this scheme based on rare-earth ion doped crystals with appropriate performance parameters. By exploiting recent advances in quantum memory lifetimes, we are able to significantly reduce system complexity while achieving high key rates, bringing global quantum networking closer to implementation.

https://doi.org/10.1364/OPTICAQ.517495

1. INTRODUCTION

Long-distance ($>10^3$ km) quantum entanglement distribution will be crucial for the development of global networked quantum computers, sensors, positioning, navigation, and timing, as well as for fundamental tests of physics. The main scientific and technical challenge is the high loss suffered by directly transmitted quantum signals that constrains the range and rate of entanglement distribution. Unlike in classical communications, deterministic amplification of quantum states is prohibited by quantum mechanics [1,2]. Currently, fiber-based long-distance quantum communication experiments are limited to approximately a few hundred to a thousand kilometers [3], made possible by new techniques such as twin-field (TF) quantum key distribution (QKD) [4,5], and developments in low-loss fiber and low-noise single photon detectors. However, going beyond $\sim 10^3$ km requires alternate approaches, such as quantum repeaters (QRs) or free-space channels via space-based platforms.

Actively corrected QRs have theoretically been shown to be capable of reaching global distances albeit with enormous technical overhead: repeater nodes, each of which contains a small-scale quantum processor, must be separated by very short distances, i.e., 1–2 km [6], due to sensitivity to link loss. QRs based on heralded generation of entanglement [7,8] can have nodes separated by several tens of kms but their total range is limited to approximately a few thousand km [8–11].

The use of free-space channels can also extend the direct-transmission limit, where fiber exponential loss scaling is replaced with the (mainly) inverse square loss scaling of free-space propagation. Recently, the Micius satellite [12] demonstrated milestones such as ground-space teleportation [13], QKD with entangled photons across 1120 km [14], intercontinental QKD operated in trusted node [15], and the integration of satellite links into long-distance, trusted node ground networks [16]. These groundbreaking achievements are however limited by line-of-sight, where the connection distance d between two ground stations is limited by the requirement to be in simultaneous view of the satellite ($d \leq 2000$ km for altitude $h = 500$ km) unless the satellite operates as a trusted node [15,17].

Fully global ($d>10^4$ km) coverage with satellites has been proposed by several groups. An initial proposal was a hybrid, space-ground QR system [18], where quantum memories (QMs) were located in ground stations. This scheme was recently extended toward fully satellite-based QRs [19,20], where the QMs are located onboard satellites [21], eliminating

intermediate trans-atmospheric quantum links. These works demonstrated that entanglement distribution across the whole globe would be possible with a network of satellites equipped with QMs and entangled photon pair sources. It was shown that a storage time of approximately <1 s would be sufficient to reach global distances [19,20], whereas intercontinental distances of >8000 km would be possible with memory times of approximately 100 ms [20,22].

An alternative to multiple QR nodes is to physically transport [23,24] entangled qubits, given sufficiently long qubit coherence times. This could be achieved via active quantum error correction [25] or with ultra-long lifetime QMs [26,27]. Here, we propose a time-delayed version of a single-node quantum repeater [28–30] that can be implemented with a single orbiting satellite carrying an ultra-long-lived QM, which we refer to as QM1, in combination with a shorter lived (~ms) QM (QM2). The addition of the lower requirement QM2 provides a feasible route toward dramatic improvements in secure key generation over QM1 alone. Using QKD as a benchmark for quantum communication [31], our scheme extends the performance and reduces the hardware requirements of a previous related proposal [26] by several orders of magnitude, especially when taking into account fine-block size effects. By improving entanglement distribution rates and reducing system complexity over previous proposals, our protocol may provide a route toward time and phase synchronization [32] and distributed quantum technologies over large distances [33,34].

This manuscript is organized as follows: we first outline the protocol with two quantum memories, highlighting differences from a previous single-memory scheme; we present finite key analysis of this scheme and derive required memory performance; finally, we discuss possible implementations of this scheme and provide an experimental guideline.

2. 2-QM TIME-DELAYED QR PROTOCOL

Global quantum communications using a low-Earth orbit (LEO) satellite equipped with a QM with a lifetime of the order of the associated orbital period (90 minutes for LEO) and an entangled photon pair source has been previously proposed [26]. The source first sends one of the photons in each entangled pair to ground station A and the other half is stored in the on-board QM. The satellite then continues in its orbit, and stored photons in the QM are retrieved and sent to ground station B as it flies over. Our scheme instead supplements a long-lived QM together with a second shorter-lived QM. QM1 needs to have $\tau_{QM1} > 1$ hour with a high multimode capacity whereas QM2 only needs $\tau_{QM2} \sim 2L/c$, where L is the range between the satellite and the ground station. Using a single QM limits the keylength scaling to η_{ch}^2 whereas a second QM enhances the scaling to $\sim \eta_{ch}$, where η_{ch} is the average single channel loss, all else being equal. Our scheme can be regarded as the time delayed version of a single quantum repeater node [28–30] that enhances the achievable key rates and tolerable losses, and eliminates the requirement for the two ground stations to be in simultaneous view.

We illustrate our scheme in Fig. 1. The protocol begins with the start of the satellite pass over ground station A and operating its entangled photon-pair source (EPS, rate s). One photon in each pair is stored in QM1, the other photon is sent to ground station A through the space-ground channel. If this transmitted photon is lost, then the corresponding stored photon in the

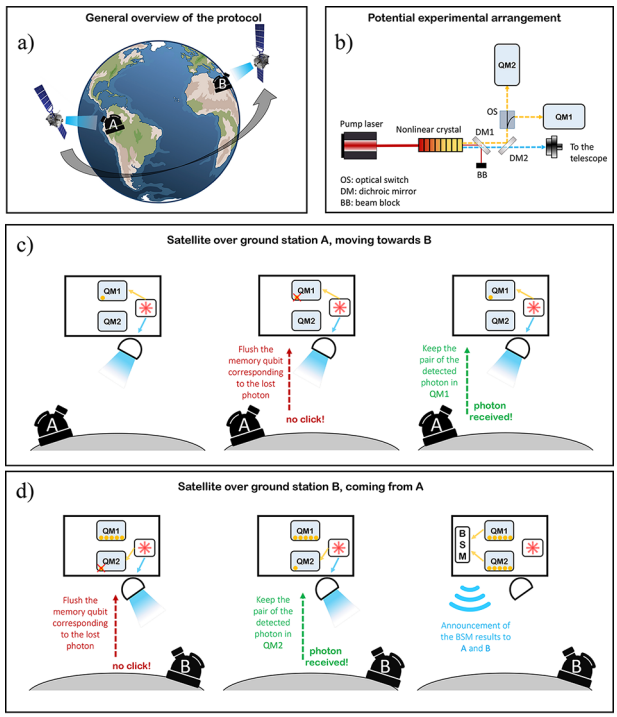

Fig. 1. 2-QM time-delayed protocol. (a) General overview of the scheme. (b) Proposed experimental setup depicting the entangled photon pair generation and absorptive memories. The photons in orange and blue modes are entangled. (c) One photon of the entangled pair is stored in the long-lived QM1, whereas its partner is sent to ground station A which informs the satellite if it was received. If ground station A does not receive the photon, the respective QM1 mode is reset and entanglement distribution is reattempted, otherwise the stored photon is kept in QM1. This continues until all storage modes of QM1 are full or the transmission window is exceeded. (d) Satellite continues in its orbit and passes close to ground station B. We use QM2 in a similar process as in panel (c) to establish shared entanglement with ground station B. Entanglement swapping is now performed by applying a BSM to the stored photons in QM1 and QM2 whose result is broadcast to ground stations A and B who may perform local unitary corrections to distill a secret key.

QM1 is erased, else the stored photon is kept if ground station A indicates successful reception. For QKD, the received photon is measured (as in BBM92 [35]) or, more generally, the ground stations could store the received photons in a QM if entanglement was required instead.

After the first overpass, the satellite continues in its orbit and the source again starts emitting entangled photon pairs when passing over ground station B. One photon of each pair is sent to ground station B whereas the other photon is stored in QM2. If ground station B successfully receives the transmitted photon, then the corresponding photon from QM2 is immediately retrieved together with a photon stored in QM1 and entanglement swapping performed by a Bell state measurement (BSM). The result of the BSM is then broadcast for local unitary corrective operations [28,29]. Although we consider a QM paired with an entangled photon pair source [10,36] as depicted in Fig. 1(b), the same protocol can be realized with a DLCZ-type memory, where the QM can emit a single photon entangled with its internal atomic states [9].

3. KEY RATE ANALYSIS

Quantum key distribution rates are often calculated in the asymptotic limit [37] assuming that statistical uncertainties can be neglected due to sufficiently large blocks sizes. However, this approximation may be invalid for limited duration overpasses, hence finite block size effects should be considered [38–43]. Here we follow the approach of Ref. [14] for the analysis of BBM92 with symmetric basis choice, due to its relative simplicity for comparative purposes. Although this analysis was refined later in Ref. [44], we assign a tighter security parameter to maintain the security of finite keys by appropriately accounting for the cost of parameter estimation.

Considering the successfully entanglement-swapped pairs shared by ground stations A and B, the finite key length in the Z basis is then given by

$$L_Z = n_Z - n_Z h\left[\frac{e_X + \sqrt{\frac{(n_Z+1)\log\left(\frac{1}{\epsilon_{\rm sec}}\right)}{2n_X(n_X+n_Z)}}}{1-\Delta}\right] - f_e n_Z h\left(e_Z\right) - n_Z\Delta - \log\frac{2}{\epsilon_{\rm corr}\epsilon_{\rm sec}^2}, \tag{1}$$

where $\epsilon_{\rm sec}$ and $\epsilon_{\rm corr}$ are secrecy and correctness levels so that the protocol is ϵ-secure if $\epsilon \geq \epsilon_{\rm sec} + \epsilon_{\rm corr}$ [14], Δ is a factor to account for the mismatch of different detector efficiencies, $n_{Z/X}$ are the number of matching and coincident Z and X basis detection events, respectively, and $e_{Z/X}$ are the quantum bit error rates (QBER) for each basis. The key length calculation for the X basis is similar to Eq. (1), thus the total key length becomes $L = L_X + L_Z$.

The QBERs with a single QR node (2 QMs) as in our protocol are given by [28]

$$e_X = \lambda_{\rm BSM}\alpha_A\alpha_B\left[\epsilon_m\left(1-\epsilon_{\rm dp}\right) + \left(1-\epsilon_m\right)\epsilon_{\rm dp}\right] + \frac{1}{2}\left[1-\lambda_{\rm BSM}\alpha_A\alpha_B\right] \tag{2}$$

and

$$e_Z = \lambda_{\rm BSM}\alpha_A\alpha_B\epsilon_m + \frac{1}{2}\left[1-\lambda_{\rm BSM}\alpha_A\alpha_B\right]. \tag{3}$$

Here $\lambda_{\rm BSM}$ is a parameter that quantifies the ideality of the BSM and it is related to the BSM fidelity $F_{\rm BSM} = \sqrt{3(\lambda_{\rm BSM}+1)/4}$; α_k is the probability of a real detection event in ground station k; ϵ_m is the misalignment error that also includes the source infidelity due to possible multi-photon excitations, and ϵ_{dp} is total dephasing during the storage in memories which depends on the individual memory errors e_m (details for both single- and double-quantum memory cases are given in Appendix A). Ensemble-based memories that we consider in this work have been shown to preserve the phase, independent of the storage time [45–47]. This is since re-emission of the stored information relies on rephasing of these excitations [48], any dephasing will result in lower operation efficiency while maintaining high fidelity. We assume a memory efficiency of $\sim$ 60% at 90 minutes following the observed $T_2 = 6$ hours in a europium-doped crystal [27,49] (see Section 4) and $\lambda_{\rm BSM} = 0.98$ [28,29] corresponding to $F_{\rm BSM} = 0.9925$. We further assume two identical passes over ground stations A and B each of 240 s duration and without memory constraints. Consequently, we will determine the required memory capacity as a result. We also do not assume a particular orbit, apart from being consistent with the overpass times and channel losses considered and achievable with realistic transmitter and receiver apertures.

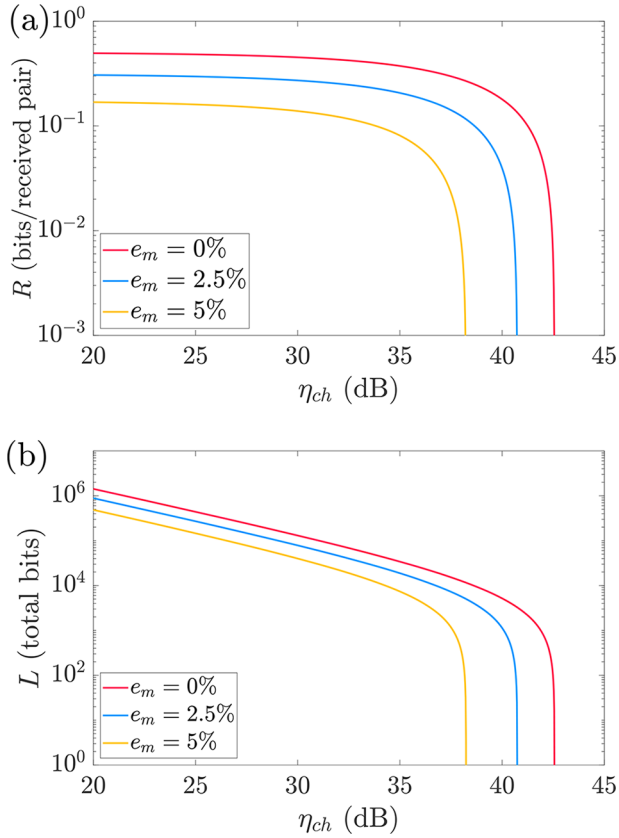

Fig. 2. 2-QM QKD performance. Overpass time 240 s consistent with a typical LEO overpass, 5 MHz source rate, average single downlink channel loss η_{ch}. (a) Secure key rate per received pair, R; (b) secure key length, L. Model parameters are given in Table 1.

Figure 2(a) shows the key rate per *received* pair, R, as a function of average single channel loss (η_{ch}), transmission periods of 240 seconds per ground station, and different memory dephasing values e_m. Since the key rate only depends on the average channel loss, this figure serves as a guide for scenarios with a given total channel loss [50]. We assume an entangled photon pair source rate $s = 5$ MHz which is mainly limited by the narrow memory bandwidth, source infidelity $\epsilon_m = 2\%$, and a tight $\epsilon_{corr} = \epsilon_{sec} = 5\times10^{-12}$ [51,52], see Appendices. We note that the pair source does not have to be deterministic as long as the required pair rate is maintained and the higher order photon components are kept low enough so that the fidelity is not degraded. We see that up to $\eta_{ch} = 42$ dB can be tolerated with two ideal QMs ($e_m = 0\%$). For $e_m = 5\%$, one can generate finite keys with single-channel loss up to 37.5 dB. For perspective, Ref. [47] reported $e_m \sim 7.5\%$ for 1 hour storage time with classical pulses. Figure 2(b) shows that finite key lengths ($L = L_X + L_Z$) of $>10^4$ can be obtained with an average single channel loss of 30 dB, such η_{ch} values have been reported in [14]. Compared with the 1-QM scheme [26], the second QM provides a marked advantage in the finite key setting (Fig. 3). Figure 3(a) shows the key rate per received pair, R, for single and double memory schemes. With a single QM, finite size effects become significant for channel losses of more than $\eta_{ch} \sim 25.9$ dB, where the crossover between 1- and 2-QM schemes happens and the maximum tolerable average loss for the 1-QM scheme is 28 dB, beyond which secure key generation is not possible in a single set of overpasses. This also means that the 1-QM scheme would

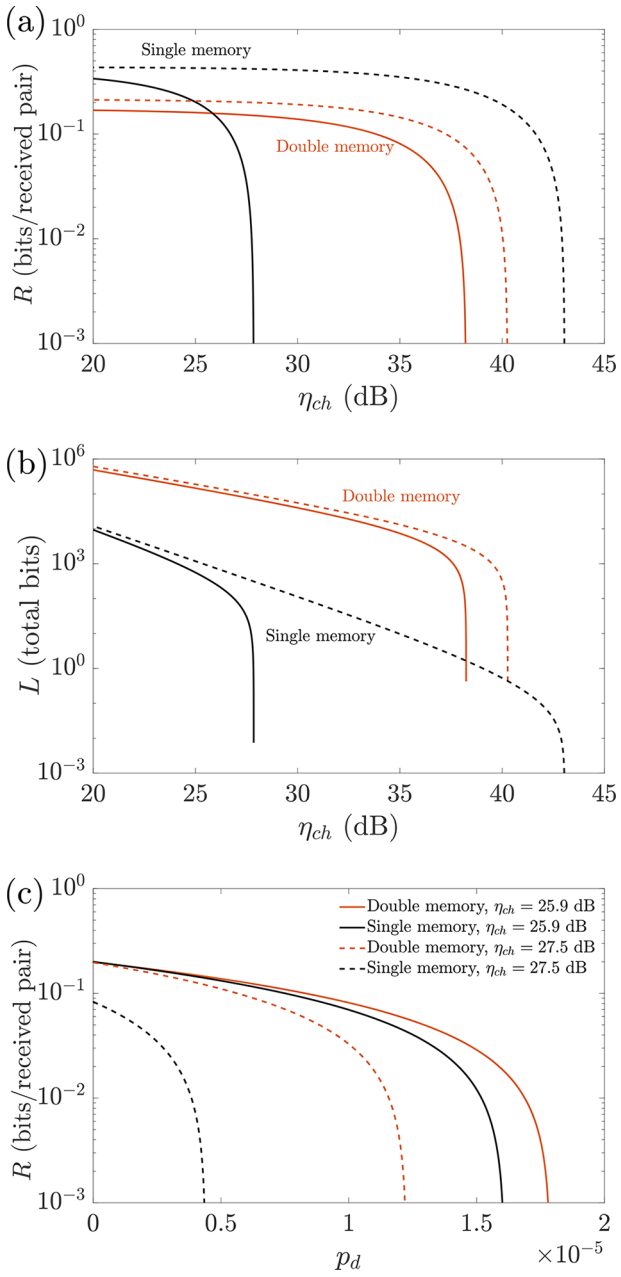

Fig. 3. Comparison of 1-QM and 2-QM key generation. (a) Finite key rate per received pair (R) for $e_m = 5\%$ (solid/dashed curves finite/asymptotic key rate); (b) total finite key length (L) as a function of average single channel loss (η_{ch}) for $e_m = 5\%$ (solid/dashed curves finite/asymptotic key length). Solid red curves in panels (a) and (b) are the same as the yellow curves in Fig. 2. (c) Finite key rate per received pair versus total incoherent noise for fixed channel losses.

not produce any finite key with channel losses such as those reported in Ref. [14]. Figure 3(b) explicitly demonstrates the advantage of the two-memory scheme, with higher loss tolerance and with up to three orders of magnitude (at approximately the crossover point for R) higher secure key lengths, L, due to the repeater effect on the second downlink indicated by the lower slope of the curve for the 2-QM case. The repeater effect in the 2-QM scheme leads to a greater number of swapped pairs between ground stations A and B, which enables the observed improvement over the 1-QM scheme.

Table 1. Reference Simulation Parameters[a]

Parameter	Symbol	Value
EPS rate	s	5 MHz
Transmission period	T	240 s
Average channel loss	η_{ch}	*See the text*
Secrecy parameter	ϵ_{sec}	5×10^{-12}
Correctness parameter	ϵ_{corr}	5×10^{-12}
Memory noise probability	p_n	1×10^{-3}
Background count probability	p_{bg}	6.4×10^{-7}
Detector dark count probability	p_{dc}	1×10^{-7}
Temporal Window	τ	200 ns
Memory efficiency	η_{mem}	0.6
Detection efficiency	η_{det}	0.8
Memory dephasing	e_m	0 – 0.05
Detector imbalance	Δ	0.02
BSM ideality	λ_{BSM}	0.98

[a]A transmission duration of 240 s over an OGS corresponds to typical LEO overpasses. Memory noise, p_n, corresponds to the probability a noise photon is emitted per storage trial. A value of $p_n = 1 \times 10^{-3}$ is consistent with current REID memories [74,75]. The assumed background count probability is consistent with nighttime operation. Daylight operations may be possible with extremely aggressive spectral filtering, diffraction-limited adaptive-optics enabled single-mode coupling, and favorable clear sky conditions and overpass geometry, though such low values may not be achievable in the majority of circumstances. However, as can been seen in Fig. 3(c), the 2-QM protocol can operate with higher p_d values for achievable single channel losses η_{ch}.

The 2-QM protocol can achieve a finite key rate that approaches its asymptotic limit even for high channel loss and contact times of only a few minutes. In contrast, the 1-QM scheme shows a 15-dB gap between the maximum tolerable loss and finite key limit due to the greatly reduced number of received pairs, without the repeater effect of the second QM, imposing a severe finite block size penalty. In the asymptotic limit, however, the single-memory scheme could in principle tolerate higher losses than the two-memory case due to a reduction of errors from the absence of a non-perfect BSM ($\lambda_{\mathrm{BSM}} = 1$ in the 1-QM case effectively) and the additional dephasing in QM2 (Appendix A). We also note that in the 2-QM case, the BSM maximum success rate of 50% (assuming passive ancilla-less static linear optics [53]) halves the number of received pairs, hence the implementation of deterministic entanglement swapping BSMs [54] could provide a tangible improvement in finite key generation and increasing loss tolerance due to longer blocks and better finite statistics.

Figure 3(c) shows the effect of incoherent detector clicks, p_d, on the key rate for $\eta_{ch} = 25.9$ dB (Appendix B), the crossover point in Fig. 3(a) between the two schemes in the finite key setting. The two-memory scheme is more resilient to noise, despite the additional errors introduced by the BSM/entanglement swapping and second memory required. This is due to the much larger block size achievable with 2-QMs leading to lower statistical uncertainties, hence tighter bounds in Eq. (1). The sensitivity on the single channel loss is also illustrated: the dashed curves for $\eta_{ch} = 27.5$ dB show that the double memory scheme has more than three times better noise tolerance than its single memory counterpart.

4. MEMORY ARCHITECTURE

For both 1-QM or 2-QM protocols, the primary memory (QM1) needs to have: (i) high multimode storage capacity, N; (ii) long storage times. For the 2-QM protocol, $N = 4(n_Z + n_X)$, where the factor of 4 arises from two contributions: (a) 50% basis mismatch between ground stations A and B; (b) assumed 50% BSM success limit. The storage time has to be larger than the orbital period (~ 90–100 min for LEO) [55]. Mode capacities of $N \sim 200$ have recently been demonstrated in several experiments: cold atoms [56] with spatial multiplexing; rare-earth-ion-doped (REID) crystal memories with temporal and spectral multiplexing [57].

REIDs have the long memory lifetime and multimode capacity required by our protocol. Due to the optically active $4f$ electronic orbitals being located within totally filled $5s$ or $5d$ shells [58], this shields them from external disturbances and results in very sharp optical lines connected to long-lived ground states. Their large inhomogenous broadening (γ_{inh}) can also be used to realize memory protocols based on rephasing of the stored excitations using the atomic frequency comb (AFC) protocol [48]. Europium REIDs have a hyperfine lifetime of approximately three weeks [59,60] with demonstrations of a coherence time of 6 hours [49], and recently the coherent storage of bright pulses for >1 hour [47]. Additionally, recent advances in developing such QMs with built-in fiber couplers [61,62] would enable enhanced coupling between the optical free space and memory modes.

The AFC protocol is a promising candidate to satisfy the strict multimode requirements of our scheme. AFC relies on creating a comb shaped absorption profile by optical pumping within the inhomogenous profile of the ensemble. It was shown that the number of temporal modes that can be stored with this protocol is $\sim N_{AFC}/6$, where N_{AFC} is the number of absorption peaks within the comb [48]. With a bandwidth of a few MHz, we can expect to create an AFC that could store $N_t \sim 10^2$ temporal modes with $N_{AFC} \sim 600$ [63]. REIDs are also suitable for large spectral multiplexing [57,64] capability due to the inhomogeneous broadening they possess: up to $N_f \sim 10^3$ spectral modes can be stored within an optical transition with $\gamma_{\text{inh}} \sim 10$ GHz. Finally, laser waveguide writing techniques [63,65] may allow the creation of $N_s \sim 100 \times 100$ arrays of spatial modes within a single crystal, thus putting the total number of available modes to $N_{\text{Mem}} = N_t \times N_f \times N_s \sim 10^9$. This hypothetical value is well beyond the required capacity of $N_{\text{QM1}} \sim 2 \times 10^6$ for 30-dB average downlink single channel loss in combination with $\eta_{mem} = 0.6$ and $\eta_{det} = 0.8$. We note that for LEO ranges and $s = 5$ MHz, we require $N_{\text{QM2}} \sim 10^5$ modes to act as a buffer taking into account the propagation delay and the need to wait for the click/no-click signal from the ground station.

These types of quantum memories require cryogenic operation at temperatures <4 K and external magnetic fields [66]. Although this is one of the technical challenges for deploying such devices in space, recent efforts to develop satellite-borne cryostats for quantum optical applications are promising [67–69]. There are also recent advances toward developing robust and miniaturized laser systems at approximately the memory wavelength of 580 nm [70]. Highly efficient, low-noise single-photon counters are also available. We should note that detector timing jitter (<1 ns) is not a significant factor as the signal photons would need to be approximately $\tau = 200$ ns long due to narrow memory linewidths. We should note that QM2 can be implemented with the same memory protocol which would also ensure the indistinguishability of photons for the BSM. The storage time and multiplexing requirements for QM2 are greatly relaxed compared with QM1. In Appendix C, we also compare the annual performance of the 2-QM protocol ($s = 5$ MHz) with a non-memory assisted continuously operating simultaneous dual-downlink from geostationary orbit ($s = 1$ GHz).

5. CONCLUSIONS

We propose a new quantum communication protocol that physically transports stored qubits in an ultra-long-lived QM (lifetime of the order of the orbital period) on an orbiting satellite, and uses a second shorter-lived QM (lifetime of the order of a round-trip classical communication signal) to substantially enhance entanglement distribution over long distances. This protocol dramatically reduces system complexity of global quantum networks by taking advantage of two different paradigms, i.e., quantum repeater behavior and physically moving qubits, eliminating the need to coordinate orbiting strings of QR satellites and multiple optical links simultaneously. Using two QMs instead of one significantly increases the maximum tolerable channel loss while reducing the required multimode capacity from $\sim 10^8$ [26] to $\sim 10^6$ despite additional errors from the second QM, a non-ideal BSM, and 50% BSM outcome inefficiency in the 2-QM case. Recent progress in QMs indicates that the necessary storage time and multimode capacity should be achievable in the near future.

These results could be improved by using more recent finite key calculations that specifically address space-based QKD scenarios. The secure key lengths may be increased by ~ 10% or else smaller block sizes could be used [44]. Wavelength division multiplexing may allow increased rates at which entangled pairs can be sent through the space-Earth quantum optical channel despite QM linewidth limitations. Finally, ultra-long-lived QMs in orbit may also serve as useful probes to investigate the intersection of quantum physics and general relativity [71] and enable human-assisted Bell tests across Earth–Moon distances [12,72,73].

There are a number of extensions to this work, including: evaluating the tradeoff between the data block sizes and the average overpass loss to maximize the finite key rate could provide requirements and specifications on quantum memory capacity and performance to support this single-node quantum repeater scheme. It may also help determine current hardware limitations to extending the protocol performance. Further, exploring the impact of different satellite overpasses on the secure key generation would elucidate the robustness of our single satellite scheme against loss and overpass duration, and inform constellation design.

APPENDIX A. KEY RATE CALCULATION DETAILS

Satellite based quantum communications present several challenges with respect to its fiber-based counterpart. These are mainly: high, dynamic channel loss, and the relatively short contact time (~min for LEO) between the sender and receiver stations. With these constraints in mind, we also take into account the finite key effects on the final, generated secure key lengths. We should stress that we base our calculations on the average single channel loss, η_{ch}, which can be achieved with many different combinations of orbital (altitude, latitude, etc.) and optical parameters (beam divergence, sender/receiver telescope apertures), for instance.

The final secure key length, $L_{X,Z}$, is given in Eq. (1). We see from Eqs. (2) and (3) that the physical factors that contribute to the QBERs, e_X and e_Z, are λ_{BSM}, α_k, ϵ_{dp}, and ϵ_m. Among these, only the memory dephasing, ϵ_{dp}, contributes to error in the X basis. Here, α_k is the probability of registering a real click in ground station k [28]. This probability then decreases with any incoherent (noise) click at the detector and depends on total detection probability η:

$$\alpha(\eta) = \frac{\eta(1-p_d)}{1-(1-\eta)(1-p_d)^2}, \tag{A1}$$

where $\eta = \eta_{ch}\eta_{det}\eta_{mem}$ with η_{ch} the average channel transmission; η_{det} the detection efficiency, and η_{mem} the combined memory write-in and read-out efficiency. The probability of any incoherent click on the detector during the detection time window is $p_d = \eta_{ch}p_n + p_{bg} + p_{dc}$, where p_n is the noise added by memory when there is no input pulse, p_{bg} is the background noise probability, and p_{dc} is detector dark count probability. These contributions are further detailed in the next section.

The efficiency mismatch between different detectors is accounted by Δ in Eq. (1). Adding a filter with small attenuation, δ_i, to the ith detector would result in $\Delta = 1 - 1/(1+\delta)$ [14]. In this work, we assume $\Delta \sim 2\%$.

The memory dephasing term, ϵ_{dp}, combines the dephasing experienced by both memories and is expressed as [28]

$$\epsilon_{dp} = e_{m1}(1-e_{m2}) + (1-e_{m1})e_{m2} \tag{A2}$$

with $e_{m1,2}$ depicting the dephasing experienced in individual memories which is assumed to be independent of the storage time as explained in the main text. With this, ϵ_{dp} becomes $2e_m(1-e_m)$ for the two- and e_m for the single-memory case, where e_m is the memory dephasing. With these, Eq. (2) becomes

$$\begin{aligned} e_X = {} & \lambda_{\mathrm{BSM}}\alpha_A\alpha_B[\epsilon_m(1-2e_m(1-e_m)) + \\ & 2e_m(1-e_m)(1-\epsilon_m)] + \frac{1}{2}[1-\lambda_{\mathrm{BSM}}\alpha_A\alpha_B], \end{aligned} \tag{A3}$$

$$e_Z = \lambda_{\mathrm{BSM}}\alpha_A\alpha_B\epsilon_m + \frac{1}{2}[1-\lambda_{\mathrm{BSM}}\alpha_A\alpha_B] \tag{A4}$$

for the two-memory, and

$$e_X = \alpha_A\alpha_B[\epsilon_m(1-e_m) + e_m(1-\epsilon_m)], \tag{A5}$$

$$e_Z = \alpha_A\alpha_B\epsilon_m + \frac{1}{2}[1-\alpha_A\alpha_B] \tag{A6}$$

for the single-memory scenarios.

APPENDIX B. INCOHERENT CLICKS

Incoherent clicks degrade the maximum tolerable loss. These arise from the following. (a) Detector dark counts, p_{dc}: dark count rate of approximately 10 Hz is readily achievable with detectors at room temperature whereas <1 Hz is possible with cryogenically cooled superconducting single photon detectors. (b) Noise coming from memory operation, p_n: long-lived QMs usually add noise to the output signal. This is due to a combination of several factors such as imperfect preparation of the memory, leakage from the strong control pulses, and resonant four wave mixing noise. The probability of emitting a noise photon per storage trial, p_n, is approximately 10^{-3} for REID QMs [74,75], whereas $\sim 10^{-4}$ has been achieved with laser cooled gases [76]. (c) Background light, p_{bg}: detailed treatment of background light under different conditions (total dark skies, full moon, daylight, etc.) is given elsewhere [22,77]. The use of adaptive optics can compensate for turbulence to allow for a diffraction limited field of view and single mode coupling, hence greatly improving background light rejection, permitting daylight satellite QKD even at 800 nm [78]. Background light can be reduced further with even narrower spectral filters (in principle, approaching the bandwidth of stored photons or lower [74,79]), though the Doppler shift due to the satellite's velocity along the line-of-sight would need to be compensated. Furthermore, one can design the photon pair source such that photons sent to the ground stations would lie within a Fraunhofer line to enable daylight operation [80]. This option would not be directly possible in a 1-QM scheme as the stored photons would later have to be transmitted to ground B, unless wavelength conversion was employed.

APPENDIX C. COMPARISON WITH A QKD FROM GEOSTATIONARY ORBIT (GEO)

Entanglement could be distributed globally with the use of high-altitude satellites simultaneously transmitting photon pairs. This requires the satellite to be sufficiently high to be in line-of-sight of the two ground stations at the same time. Following Refs. [20,81], in this section, we present calculations of entanglement-based QKD (ent-QKD) without any QMs from a satellite in GEO (see Ref. [82] for a similar analysis) at an altitude of 36×10^3 km with different receiver telescope diameters. We assume a source rate of 1 GHz, sender telescope diameter of 0.3 m, $p_d = 10^{-6}$, wavelength of 852 nm (atmospheric transmissivity at 852 nm is approximately 25% higher than it is at 580 nm [20]) and beam divergence of 5 μrad. We follow our earlier work [20,22] for the channel modeling. This calculation does not include pointing and tracking errors or turbulence effects, thus represents a best case link loss scenario.

With this, we see that losses prevent achieving fully global distances, even with 2.5-m diameter receiver telescopes. To compare this GEO scenario with the presented protocol in this manuscript, one needs to calculate the number of flyovers over a given pair of ground stations. Along these lines, in Ref. [26], a hypothetical link between Adelaide and Brussels (total distance 15.9×10^3 km) is considered for which the authors find 1257 flyover pairs within a year. According to Fig. 2(b), each of these passes can generate finite key lengths up to 10^4 with average single channel loss of 35 dB. Our analysis shows that deploying

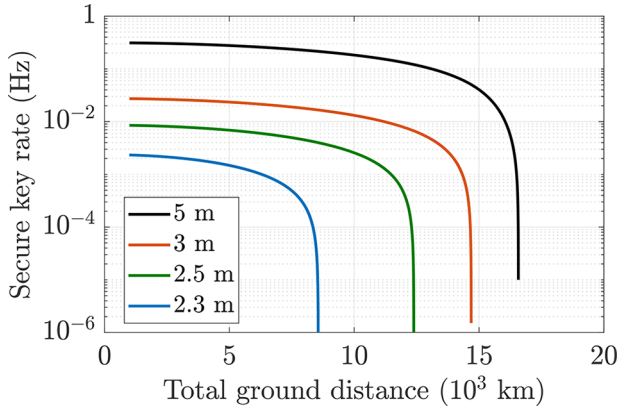

Fig. 4. Achievable key rates from a GEO with an ent-QKD protocol without any QM with different receiver telescope diameters. Other parameters are given in Appendix C.

a single satellite equipped with an ultra-long lifetime QM using the protocol in this manuscript would result in a performance gain of $\sim 2.5 \times 10^2$ over the GEO scenario per Fig. 4.

Funding. Innovate UK (EP/S000364/1); UK Space Agency (NSTP3- FT-063 NTSP Fast Track "System Integration & Testing of a CubeSat WCP QKD Payload to TRL5"); Engineering and Physical Sciences Research Council (EP/M013472/1, EP/T001011/1, EP/T517288/1, EP/W027011/1); European Cooperation in Science and Technology (CA15220); Deutsches Zentrum für Luft- und Raumfahrt (50WM1958, 50WM2055, 50WM2347); European Union H2020 Marie Skłodowska-Curie Actions (894590).

Acknowledgments. We thank S. Wittig for bringing the earlier work [26] to our attention during discussion at an early stage of this work and E. İmre for useful discussions on satellite communication techniques.

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. D. Dieks, "Communication by EPR devices," Phys. Lett. A **92**, 271–272 (1982).
2. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).
3. J.-P. Chen, C. Zhang, Y. Liu, *et al.*, "Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km," Phys. Rev. Lett. **124**, 070501 (2020).
4. M. Lucamarini, Z. L. Yuan, J. F. Dynes, *et al.*, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).
5. Y. Liu, W.-J. Zhang, C. Jiang, *et al.*, "Experimental twin-field quantum key distribution over 1000 km fiber distance," Phys. Rev. Lett. **130**, 210801 (2023).
6. S. Muralidharan, J. Kim, N. Lütkenhaus, *et al.*, "Ultrafast and fault-tolerant quantum communication across long distances," Phys. Rev. Lett. **112**, 250501 (2014).
7. L. Childress, J. M. Taylor, A. S. Sørensen, *et al.*, "Fault-tolerant quantum communication based on solid-state photon emitters," Phys. Rev. Lett. **96**, 070504 (2006).
8. N. Sangouard, C. Simon, H. de Riedmatten, *et al.*, "Quantum repeaters based on atomic ensembles and linear optics," Rev. Mod. Phys. **83**, 33–80 (2011).
9. L.-M. Duan, M. D. Lukin, J. I. Cirac, *et al.*, "Long-distance quantum communication with atomic ensembles and linear optics," Nature **414**, 413–418 (2001).
10. C. Simon, H. de Riedmatten, M. Afzelius, *et al.*, "Quantum repeaters with photon pair sources and multimode memories," Phys. Rev. Lett. **98**, 190503 (2007).
11. S. E. Vinay and P. Kok, "Practical repeaters for ultralong-distance quantum communication," Phys. Rev. A **95**, 052336 (2017).
12. C.-Y. Lu, Y. Cao, C.-Z. Peng, *et al.*, "Micius quantum experiments in space," Rev. Mod. Phys. **94**, 035001 (2022).
13. J.-G. Ren, P. Xu, H.-L. Yong, *et al.*, "Ground-to-satellite quantum teleportation," Nature **549**, 70–73 (2017).
14. J. Yin, Y.-H. Li, S.-K. Liao, *et al.*, "Entanglement-based secure quantum cryptography over 1,120 kilometres," Nature **582**, 501–505 (2020).
15. S.-K. Liao, W.-Q. Cai, J. Handsteiner, *et al.*, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett. **120**, 030501 (2018).
16. Y.-A. Chen, Q. Zhang, T.-Y. Chen, *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature **589**, 214–219 (2021).
17. T. Vergoossen, S. Loarte, R. Bedington, *et al.*, "Modelling of satellite constellations for trusted node QKD networks," Acta Astronaut. **173**, 164–171 (2020).
18. K. Boone, J.-P. Bourgoin, E. Meyer-Scott, *et al.*, "Entanglement over global distances via quantum repeaters with satellite links," Phys. Rev. A **91**, 052325 (2015).
19. C. Liorni, H. Kampermann, and D. Bruß, "Quantum repeaters in space," New J. Phys. **23**, 053021 (2021).
20. M. Gündoğan, J. S. Sidhu, V. Henderson, *et al.*, "Proposal for space-borne quantum memories for global quantum networking," npj Quant. Inf. **7**, 128 (2021).
21. E. Da Ros, S. Kanthak, E. Sağlamyürek, *et al.*, "Proposal for a long-lived quantum memory using matter-wave optics with Bose-Einstein condensates in microgravity," Phys. Rev. Res. **5**, 033003 (2023).
22. J. Wallnöfer, F. Hahn, M. Gündoğan, *et al.*, "Simulating quantum repeater strategies for multiple satellites," Commun. Phys. **5**, 169 (2022).
23. W. Li, P. Islam, and P. Windpassinger, "Controlled transport of stored light," Phys. Rev. Lett. **125**, 150501 (2020).
24. Z.-Q. Zhou, D.-L. Chen, M. Jin, *et al.*, "A transportable long-lived coherent memory for light pulses," Science Bulletin **67**, 2402–2405 (2022).
25. S. J. Devitt, A. D. Greentree, A. M. Stephens, *et al.*, "High-speed quantum networking by ship," Sci. Rep. **6**, 36163 (2016).
26. S. E. Wittig, S. M. Wittig, A. Berquanda, *et al.*, "Concept for single-satellite global quantum key distribution using a solid state quantum memory," http://iafastro.directory/iac/paper/id/36863/summary/ (2017). IAC-17,B2,7,1,x36863.
27. J. Bland-Hawthorn, M. J. Sellars, and J. G. Bartholomew, "Quantum memories and the double-slit experiment: implications for astronomical interferometry," J. Opt. Soc. Am. B **38**, A86–A98 (2021).
28. D. Luong, L. Jiang, J. Kim, *et al.*, "Overcoming lossy channel bounds using a single quantum repeater node," Appl. Phys. B **122**, 96 (2016).
29. R. Trényi and N. Lütkenhaus, "Beating direct transmission bounds for quantum key distribution with a multiple quantum memory station," Phys. Rev. A **101**, 012325 (2020).
30. S. Langenfeld, P. Thomas, O. Morin, *et al.*, "Quantum repeater node demonstrating unconditionally secure key distribution," Phys. Rev. Lett. **126**, 230506 (2021).
31. P. K. Tysowski, X. Ling, N. Lütkenhaus, *et al.*, "The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD)," Quantum Sci. Technol. **3**, 024001 (2018).
32. J. Shi and S. Shen, "A clock synchronization method based on quantum entanglement," Sci. Rep. **12**, 10185 (2022).
33. J. S. Sidhu and P. Kok, "Geometric perspective on quantum parameter estimation," AVS Quantum Science **2**, 014701 (2020).
34. X. Guo, C. R. Breum, J. Borregaard, *et al.*, "Distributed quantum sensing in a continuous-variable entangled network," Nat. Phys. **16**, 281–284 (2020).
35. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557–559 (1992).
36. J. V. Rakonjac, D. Lago-Rivera, A. Seri, *et al.*, "Entanglement between a telecom photon and an on-demand multimode solid-state quantum memory," Phys. Rev. Lett. **127**, 210502 (2021).
37. S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography," Adv. Opt. Photonics **12**, 1012–1236 (2020).
38. J. S. Sidhu, S. K. Joshi, M. Gündoğan, *et al.*, "Advances in space quantum communications," IET Quantum Communication **2**, 182–217 (2021).
39. T. Islam, J. S. Sidhu, B. L. Higgins, *et al.*, "Finite resource performance of small satellite-based quantum key distribution missions," (2022).
40. J. S. Sidhu, T. Brougham, D. McArthur, *et al.*, "Key generation analysis for satellite quantum key distribution", in *Quantum Technology: Driving Commercialisation of an Enabling Science II*, Vol. 11881 M. J. Padgett, K. Bongs, A. Fedrizzi, and A. Politi, eds., International Society for Optics and Photonics (SPIE, 2021), pp. 1–8.
41. J. S. Sidhu, T. Brougham, D. McArthur, *et al.*, "Finite key effects in satellite quantum key distribution," npj Quantum Information **8**, 18 (2022).
42. J. S. Sidhu, T. Brougham, D. McArthur, *et al.*, "Finite key performance of satellite quantum key distribution under practical constraints," Commun. Phys. **6**, 210 (2023).
43. J. S. Sidhu, T. Brougham, D. McArthur, *et al.*, "Satellite quantum key distribution performance analysis and optimization with finite

key size constraints", in *Quantum Computing, Communication, and Simulation III*, Vol. 12446 (SPIE, 2023), pp. 129–137.
44. C. C.-W. Lim, F. Xu, J.-W. Pan, *et al.*, "Security analysis of quantum key distribution with small block length and its application to quantum space communications," Phys. Rev. Lett. **126**, 100501 (2021).
45. M. U. Staudt, M. Afzelius, H. de Riedmatten, *et al.*, "Interference of multimode photon echoes generated in spatially separated solid-state atomic ensembles," Phys. Rev. Lett. **99**, 173602 (2007).
46. M. Gündoğan, M. Mazzera, P. M. Ledingham, *et al.*, "Coherent storage of temporally multimode light using a spin-wave atomic frequency comb memory," New J. Phys. **15**, 045012 (2013).
47. Y. Ma, Y.-Z. Ma, Z.-Q. Zhou, *et al.*, "One-hour coherent optical storage in an atomic frequency comb memory," Nat. Commun. **12**, 2381 (2021).
48. M. Afzelius, C. Simon, H. de Riedmatten, *et al.*, "Multimode quantum memory based on atomic frequency combs," Phys. Rev. A **79**, 052329 (2009).
49. M. Zhong, M. P. Hedges, R. L. Ahlefeldt, *et al.*, "Optically addressable nuclear spins in a solid with a six-hour coherence time," Nature **517**, 177–180 (2015).
50. The exact channel loss will depend on the specifics of the system, e.g. transmitter and receiver aperture, wavelength, overpass geometry, but for the purposes of a comparison between the two different memory configurations, these have been abstracted away as they should not alter the relative performance.
51. According to Ref. [44,52], when corrected, this corresponds to a larger security parameter of around 10^{-9}.
52. M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," Quantum **1**, 14 (2017).
53. H. A. Zaidi and P. van Loock, "Beating the one-half limit of ancilla-free linear optics Bell measurements," Phys. Rev. Lett. **110**, 260501 (2013).
54. M. Riebe, T. Monz, K. Kim, *et al.*, "Deterministic entanglement swapping with an ion-trap quantum computer," Nat. Phys. **4**, 839–842 (2008).
55. Half an orbital period would be sufficient to ensure that antipodal points on the Earth could be connected by a pair of consecutive overpasses, but this requires that the satellite ground track passes close by each station within a single orbit. Generally, a satellite may take several orbits to overfly one ground station and then the other, hence even longer storage times would allow for more opportunities for entanglement distribution between a network of ground stations.
56. Y.-F. Pu, N. Jiang, W. Chang, *et al.*, "Experimental realization of a multiplexed quantum memory with 225 individually accessible memory cells," Nat. Commun. **8**, 15359 (2017).
57. A. Seri, D. Lago-Rivera, A. Lenhard, *et al.*, "Quantum storage of frequency-multiplexed heralded single photons," Phys. Rev. Lett. **123**, 080502 (2019).
58. P. Goldner, A. Ferrier, and O. Guillot-Noël, *Chapter 267 - Rare Earth-Doped Crystals for Quantum Information Processing*, Vol. 46 of Handbook on the Physics and Chemistry of Rare Earths (Elsevier, 2015).
59. F. Könz, Y. Sun, C. W. Thiel, *et al.*, "Temperature and concentration dependence of optical dephasing, spectral-hole lifetime, and anisotropic absorption in Eu^{3+}:Y_2SiO_5," Phys. Rev. B **68**, 085109 (2003).
60. B. Lauritzen, N. Timoney, N. Gisin, *et al.*, "Spectroscopic investigations of Eu^{3+}:Y_2SiO_5 for quantum memory applications," Phys. Rev. B **85**, 115111 (2012).
61. J. V. Rakonjac, G. Corrielli, D. Lago-Rivera, *et al.*, "Storage and analysis of light-matter entanglement in a fiber-integrated system," Sci. Adv. **8**, eabn3919 (2022).
62. D.-C. Liu, P.-Y. Li, T.-X. Zhu, *et al.*, "On-demand storage of photonic qubits at telecom wavelengths," Phys. Rev. Lett. **129**, 210501 (2022).
63. M.-X. Su, T.-X. Zhu, C. Liu, *et al.*, "On-demand multimode optical storage in a laser-written on-chip waveguide," Phys. Rev. A **105**, 052432 (2022).
64. N. Sinclair, E. Saglamyurek, H. Mallahzadeh, *et al.*, "Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control," Phys. Rev. Lett. **113**, 053603 (2014).
65. G. Corrielli, A. Seri, M. Mazzera, *et al.*, "Integrated optical memory based on laser-written waveguides," Phys. Rev. Appl. **5**, 054013 (2016).
66. D. L. McAuslan, J. G. Bartholomew, M. J. Sellars, *et al.*, "Reducing decoherence in optical and spin transitions in rare-earth-metal-ion–doped materials," Phys. Rev. A **85**, 032339 (2012).
67. J. R. Olson, P. Champagne, E. Roth, *et al.*, "Microcryocooler for tactical and space applications," AIP Conf. Proc. **1573**, 357–364 (2014).
68. L. You, J. Quan, Y. Wang, *et al.*, "Superconducting nanowire single photon detection system for space applications," Opt. Express **26**, 2965–2971 (2018).
69. H. Dang, T. Zhang, R. Zha, *et al.*, "Development of 2-K space cryocoolers for cooling the superconducting nanowire single photon detector," IEEE Trans. Appl. Supercond. **29**, 1–4 (2019).
70. A. Sahm, N. Werner, J. Hofmann, *et al.*, "Compact miniaturized laser module emitting more than 1.6 w of yellow light at 576 nm," IEEE Photonics Technol. Lett. **30**, 1878–1881 (2018).
71. R. Barzel, M. Gündogan, M. Krutzik, *et al.*, "Gravitationally induced entanglement dynamics of photon pairs and quantum memories," *Quantum* 8, (2024).
72. M. Gündogan, T. Jennewein, F. K. Asadi, *et al.*, "Topical white paper: A case for quantum memories in space," arXiv, arXiv:2111.09595 (2021).
73. J.-M. Mol, L. Esguerra, M. Meister, *et al.*, "Quantum memories for fundamental science in space," Quantum Sci. Technol. **8**, 024006 (2023).
74. M. Gündoğan, P. M. Ledingham, K. Kutluer, *et al.*, "Solid state spin-wave quantum memory for time-bin qubits," Phys. Rev. Lett. **114**, 230501 (2015).
75. A. Ortu, A. Holzäpfel, J. Etesse, *et al.*, "Storage of photonic time-bin qubits for up to 20 ms in a rare-earth doped crystal," npj Quantum Inf. **8**, 29 (2022).
76. L. Heller, J. Lowinski, K. Theophilo, *et al.*, "Raman storage of quasi-deterministic single photons generated by Rydberg collective excitations in a low-noise quantum memory," Phys. Rev. Appl. **18**, 024036 (2022).
77. M. Er-long, H. Zheng-fu, G. Shun-sheng, *et al.*, "Background noise of satellite-to-ground quantum key distribution," New J. Phys. **7**, 215 (2005).
78. M. T. Gruneisen, M. L. Eickhoff, S. C. Newey, *et al.*, "Adaptive-optics-enabled quantum communication: a technique for daytime space-to-Earth links," Phys. Rev. Appl. **16**, 014067 (2021).
79. S. E. Beavan, E. A. Goldschmidt, and M. J. Sellars, "Demonstration of a dynamic bandpass frequency filter in a rare-earth ion-doped crystal," J. Opt. Soc. Am. B **30**, 1173–1177 (2013).
80. M. Abasifard, C. Cholsuk, R. G. Pousa, *et al.*, "The ideal wavelength for daylight free-space quantum key distribution," (2023).
81. X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," Phys. Rev. A **76**, 012307 (2007).
82. B. Dirks, I. Ferrario, A. Le Pera, *et al.*, "GEOQKD: quantum key distribution from a geostationary satellite", in *International Conference on Space Optics-ICSO 2020*, Vol. 11852 (SPIE, 2021), pp. 222–236.