ARTICLE   OPEN

Check for updates

Towards metropolitan free-space quantum networks

Andrej Kržič [1,2 ✉], Sakshi Sharma[1,2], Christopher Spiess [1,2], Uday Chandrashekara[1,2], Sebastian Töpfer [1], Gregor Sauer[1,2], Luis Javier González-Martín del Campo[1,2], Teresa Kopf[1], Stefan Petscharnig [3], Thomas Grafenauer[3], Roland Lieger[3], Bernhard Ömer[3], Christoph Pacher [3,4], René Berlich [1], Thomas Peschel[1], Christoph Damm[1], Stefan Risse[1], Matthias Goy[1], Daniel Rieländer[1], Andreas Tünnermann[1,2,5] and Fabian Steinlechner [1,2 ✉]

Quantum communication has seen rapid progress towards practical large-scale networks, with quantum key distribution (QKD) spearheading this development. While fibre-based systems have been shown to be well suited for metropolitan scales, suitable fibre infrastructure may not always be in place. Here, we make the case for an entanglement-based free-space quantum network as a practical and efficient alternative for metropolitan applications. We developed a deployable free-space QKD system and demonstrated its use in realistic scenarios. For a representative 1.7-km free-space link, we showcase its ad hoc deployability and achieve secure key rates of up to 5.7 kbps, with 2.5 kbps in direct noon sunlight. By extrapolating experimental data, we show that kbps key rates are achievable even for 10-km distances and multi-user scenarios. We anticipate that our work will establish free-space networks as a viable solution for metropolitan applications and an indispensable complementary building block in the future global quantum internet.

INTRODUCTION

The core functionality of a quantum communication network is to distribute quantum information between two or more parties[1]. Many revolutionizing applications of quantum networks have already been identified and a roadmap towards full-blown quantum internet has been proposed[2]. While there are still many uncertainties as to the technological platforms that will ultimately make up the quantum internet, one thing is clear: it will be a heterogeneous network of various special-purpose sub-networks that employ different types of links and interconnects.

Quantum key distribution (QKD) networks have so far been the driving force for this development[3]. Although certainly not the only networks of interest, they have been paving the way also for other distributed quantum information processing protocols. For this reason, achievable secure key rates have often been used to benchmark the level of technological maturity of quantum networks in general. Currently, connecting many users distributed over large distances requires trusted nodes[4], which comes with the price of losing any possibility of end-to-end security. Unlocking the full quantum advantage in global-scale networks is therefore an ongoing challenge. A substantial proportion of current research is focused on extending the reach of individual quantum links, either through satellites[5–9] or fibre-based quantum repeaters[10–12].

Over shorter, metropolitan-scale distances, where end-to-end quantum state transmission is more easily achieved, the research focus is on a different set of challenges. One of the primary concerns is the question of scalability, i.e. how to increase the number of users in a network[13–16]. Another line of research aims to make metropolitan quantum network technology more accessible, flexible, and deployable[17–20]. An important challenge is also to interconnect networks based on different physical platforms[21]. However, all this progress is made almost exclusively with optical fibre links.

In some metropolitan application scenarios, end-to-end fibre links are not feasible. A possible alternative are terrestrial free-space links. These are still far behind the technological maturity of fibre-based systems, particularly in terms of the availability of off-the-shelf and plug-and-play solutions that are required for their deployment. Free-space links face additional challenges, such as link alignment, atmospheric turbulence, and daylight noise[22].

In the following, we argue that entanglement distribution is particularly well-suited to metropolitan-scale networks. Among the plethora of prepare-and-measure implementations, however, only a handful of groups has performed entanglement-based QKD over terrestrial free-space links[23–33], of which merely two were performed in daylight (see Supplementary Note 1 for a detailed review). Note, that many of these experiments explicitly aimed at advancing technology towards satellite deployment, while the specific challenges of readily deployable terrestrial networks were rarely addressed. Secure key rates in the order of hundreds of bits per second (bps) have been achieved over kilometre distances at night[24,28], while in daylight, similar rates have been demonstrated over a distance of only 350 m[27]. It has therefore been widely argued that the entanglement-based approach lacks the techno-logical maturity and applicability of alternative approaches[34–38].

Here, we make the case for a metropolitan free-space network architecture that can be deployed to secure communication at summits, conferences, and other events, or complement an existing network infrastructure whenever end-to-end fibre con-nections are not available. The architecture is built around a central entanglement server that streams entangled photons to users on the network. We developed the key building blocks of this architecture, including: a portable high-visibility entangled photon pair source, deployable and efficient free-space terminals
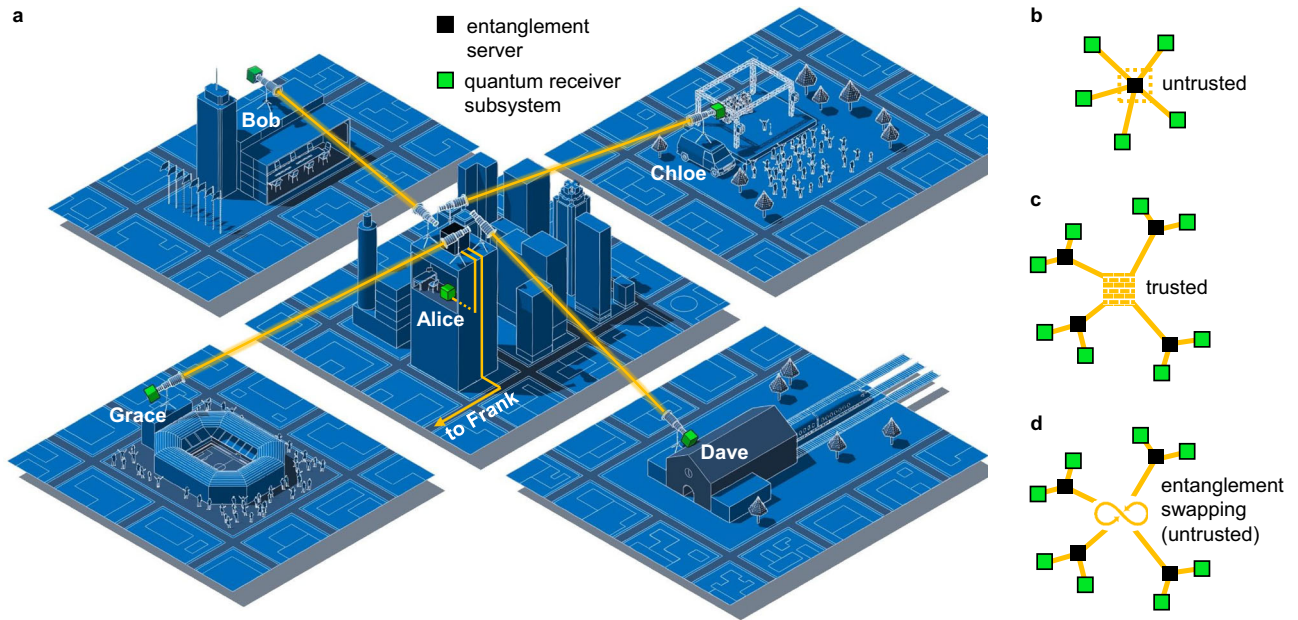
Fig. 1 Metropolitan entanglement-based free-space network. a A standardized centrally located entanglement server (ES, black box) is streaming entangled photons into the network. Free-space channels are used to connect distant buildings and parts of a metropolitan area, while fibre connections may still be used in a complementary way, for example, to connect to offices within the central building. Each end user owns an application-specific quantum receiver subsystem (green boxes). **b** The corresponding physical layer network topology. At the quantum communication layer, the network is a pairwise connected mesh, so that every end user can communicate with any other (not shown). **c** A near-term extension possibility using several ESs and a central trusted node. **d** Eventually, by introducing entanglement swapping, the trusted node could again be turned into an untrusted one, while the overall network topology would remain unchanged.

that are specifically designed for metropolitan applications, and compact and passive quantum state analysis and detection with dedicated filtering for daytime operation. To demonstrate the competitiveness of this approach in terms of efficiency, we benchmark its key generation capacity in several link configurations. We performed QKD experiments in realistic metropolitan scenarios: over a 1.7-km link to a temporary container atop another building and between two government offices separated by 300 m, showcasing its capability of providing ad hoc quantum security. We demonstrated record kbps rates are achievable in nighttime as well as in broad daylight. Finally, we provide estimates of key rates for longer 10-km links and for scenarios with multiple free-space links.

RESULTS

Entanglement-based quantum network

We consider a network architecture, where an entangled photon source acts as a server that streams entanglement into a metropolitan-scale network consisting of free-space links (Fig. 1a). The natural choice for placing the entanglement server (ES) is a central high-rise building with a clear line of sight to the relevant urban areas. Each of the end users owns a quantum receiver subsystem (QRS), which typically incorporates quantum state analysis and detection, timing and synchronization electronics, and post-processing software. Although the network has a star topology at the physical layer (Fig. 1b), recently proposed multiplexing strategies can leverage the nonlocal correlations of entangled pairs to provide a fully connected mesh network at the quantum communication layer[13,16,20].

Employing quantum entanglement as the main network resource has several key advantages over the more established prepare-and-measure schemes. Entanglement offers additional layers of security via the prospect of device-independent protocols[39]. The ES can thus act as an untrusted relay node and

lift the requirement for direct line of sight between the transceiver telescopes of any two users. Furthermore, the ES is all passive, meaning that the post-processing is delegated downstream to the user, which allows for standardization of ES, while the users can use an application-specific QRS. This gives a large degree of flexibility and even upgradeability, as more advanced schemes, protocols, and post-processing methods become available over time. Moreover, entanglement quite naturally supports many other promising applications beyond QKD[22].

The network size and reach can be readily extended by introducing several ESs, all interconnected through a central trusted node and each distributing entanglement to end users in their own local areas (Fig. 1c). In a more distant future, the requirement for trusting the central node could eventually be lifted by introducing entanglement swapping[40], without changing the physical network topology (Fig. 1d). As indicated in Fig. 1a, the architecture is also not limited to free-space links—the ES can act as a convenient interface between a free-space and a fibre link segment, for example, to connect a metropolitan free-space network to the fibre backbone of a larger intercity network.

Deployable free-space QKD system

We developed a quantum communication system specifically suited for metropolitan applications. It consists of all the key building blocks necessary to implement the present free-space quantum network and can be fully deployed at a new site in less than a day, without requiring prior infrastructure apart from access to electricity. The system is schematically shown in Fig. 2 and resembles the Alice-Bob segment of the network in Fig. 1a. Our ES generates pairs of polarization-entangled photons at 810 nm (Methods), of which one is sent to Alice via a single-mode fibre, while the other one is sent to Bob using a free-space link. For fine alignment of the free-space link and beam stabilization, we use a 1064 nm beacon laser beam, which co-propagates along the signal photons from Alice to Bob. Analysis of the beacon beam at
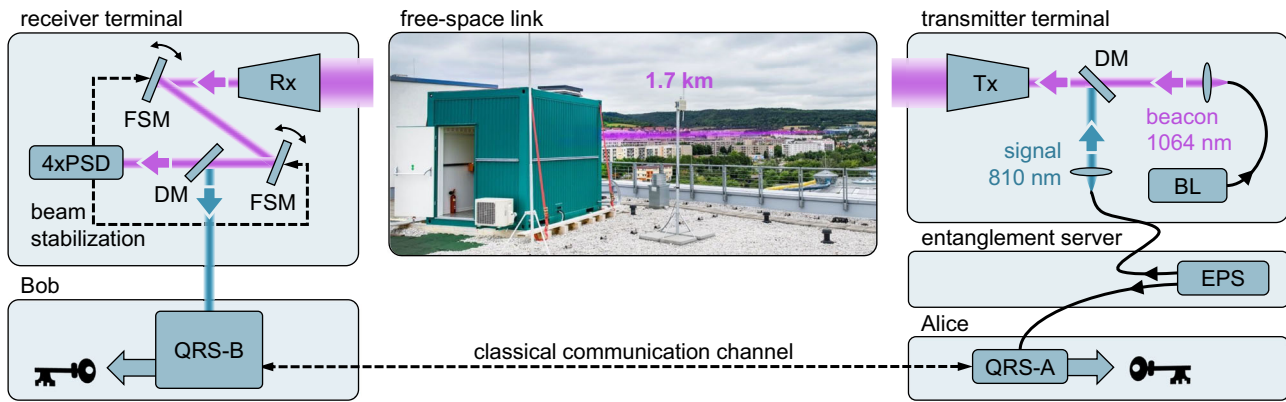
Fig. 2 Experimental setup. An entangled photon source (EPS) acts as a server that generates pairs of polarization-entangled photons at 810 nm. One photon of each pair is sent to Alice via a single-mode fibre, while the other one is sent to Bob via a free-space link spanned by a transmitter and a receiver telescope (Tx and Rx). A 1064 nm beacon laser (BL) creates a reference beam that is combined with the quantum signal at a dichroic mirror (DM) and co-propagates with it over the free-space link. At Bob, the beacon beam is analyzed in a dedicated module consisting of four position sensitive detectors (4xPSD), which generates feedback signal for two fast-steering mirrors (FSM) that in turn stabilize the beam. Both Alice and Bob own a quantum receiver subsystem (QRS-A and QRS-B) for generating the secret key. Optical elements that are irrelevant for the present experiment have been left out for clarity here. The free-space link shown here is the 1.7-km link in Jena, Germany, between Fraunhofer IOF and Stadtwerke Jena.

Bob provides a feedback signal for two fast steering mirrors, which in turn counteract fluctuations and stabilize the free-space channel in the presence of atmospheric turbulence and mechanical system instabilities. The use of a closed-loop beam stabilization system enables long-term operation and also facilitates the use of a spatial filter with a small field of view at Bob, which is necessary for daylight operation of the system (Methods).

Both Alice and Bob own a quantum receiver subsystem (QRS), which we developed for performing QKD with the BBM92 protocol[41] (Methods). Bob's QRS further incorporates specially designed spectral and spatial filtering modules for daylight operation. Alice's QRS, on the other hand, does not require dedicated filtering of daylight noise, since it is not directly exposed to the free-space link. Bob's QRS is also equipped with a motorized polarization controller that allows for automated alignment of the polarization frame of reference with Alice. The classical channel between Alice and Bob's QRS is realized with commercial radio antennas.

System performance in night and day
Using our system, we established a quantum link in Jena, Germany, between Fraunhofer IOF and a temporary container on top of a 1.7 km distant public service building. In Fig. 3, we benchmark the system performance in terms of quantum bit error rate (QBER) and achievable secure key rate (SKR) for two experiments that cover two extremes of link conditions: nighttime, when the background noise is negligible and the atmospheric turbulence weaker, and daytime, when solar radiation introduces considerable background noise and the turbulence is typically stronger[42]. For reference, we also show Bob's detected count rates, which are further split into signal and background noise contributions (Methods), as well as solar radiation measured by a weather station.

During the night experiment on 2 March 2022, we demonstrated a stable performance with QBER of less than 2%, resulting in an average SKR of 5.4 kbps over several hours. During the daytime experiment on 25 February 2022, however, the system performance varied to a much greater extent. At the beginning of this experiment, right before noon, the link was exposed to direct sunlight, i.e. no clouds were blocking the Sun as seen from the link (see Supplementary Note 4). During these conditions that lasted roughly half an hour, the detected noise rates reached values larger than 400 kcps and were up to 3.8-times higher than the

detected signal rates, despite strong spectral and spatial filtering. Nevertheless, the resulting QBER was kept below 3.4% and the SKR above 2.5 kbps, thanks to the further strong temporal filtering allowed by the tight temporal correlations of entangled photons. Over the next few hours, small clouds sporadically blocked the Sun, in turn reducing the background noise and restoring the system performance. Furthermore, we can see a clear correlation between the background photon rates and the independently measured solar radiation, and that the system performance varies as a direct consequence of sunlight. The only exception is the last drop of performance that happened after 14:00, which was not due to daylight but due to a sudden drop of the ES output, which is indicated by the simultaneous sharp drop of detected signal rates at Bob (Fig. 3) and at Alice (see Supplementary Note 5).

We note that unlike for spatial filtering, the full potentials of spectral and temporal filtering were not exploited in daytime experiments. Optimizing the spectral filter bandwidth and coincidence window could substantially increase system resilience to daylight noise and increase the achievable secure key rates. The reported secure key rates are ε-secure with $\varepsilon < 10^{-10}$ (Methods), however, even security of $\varepsilon < 10^{-20}$ could be achieved by sacrificing only about 0.1 kbps of SKR (see Supplementary Note 6).

We extrapolated our measurements to estimate achievable secure key rates for longer links and multi-user scenarios (Methods). By taking the experimental data from our night experiment and considering the additional loss in Bob's channel as estimated for a 10-km link, we arrive at SKR of 3.3 kbps. For a similar extrapolation of the daytime experiment data, scaling of the background noise rates on the distance would need to be further considered, which is beyond the scope of this work.

To gauge the performance in other link configurations, we simulate a scenario, consisting of two independent 1.7-km free-space links from the ES to Alice and Bob (Methods). Extrapolation of experimental data obtained during the night experiment shows that a SKR of more than 1.1 kbps would be possible. However, for the case of direct exposure of both links to sunlight, optimization of filtering parameters in all degrees of freedom would be required. For example, a 3-fold decrease of the spectral filter bandwidth to 1 nm would result in a SKR of more than 200 bps and optimization of the coincidence window offers further space for improvement. These estimates apply also to a general multi-user scenario based on wavelength division multiplexing, where each of the users is separated by an identical 1.7-km free-space
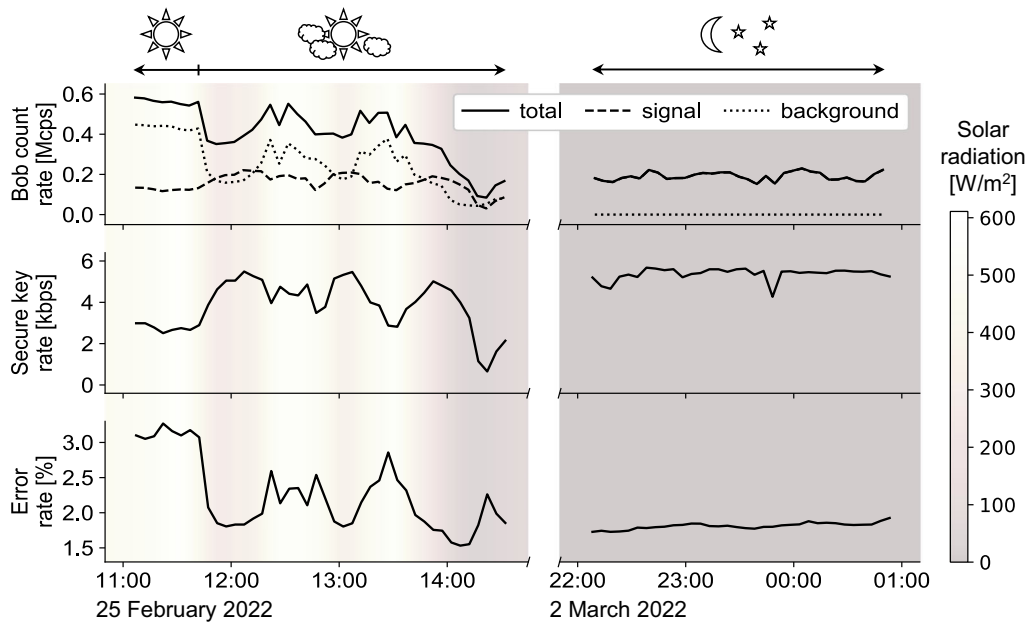
Fig. 3 Demonstration of free-space quantum key distribution. Single photon count rates at Bob, quantum bit error rates, and the corresponding secure key rates are shown for different link conditions. The daytime experiment (left) started around noon, with the link fully exposed to direct sunlight. It then continued with a sporadic decrease and increase of sunlight due to the moving clouds. During the night experiment (right), the background noise was negligible, resulting in a much more stable performance. The plotted values are 5-min averages and the horizontal axis shows the local time of day. The background colour corresponds to the solar radiation measured independently by a weather station (solar radiation data: University of Applied Sciences Jena).

link from the ES, assuming a perfect and uniform partition of the ES emission spectrum into the multiplexed channels (Methods).

Finally, we note that in July 2021, we deployed the system to establish a free-space QKD link between two 300 m separated government offices in Bonn, Germany, where we achieved similar key rates in night and in full daylight.

DISCUSSION

We proposed an entanglement-based free-space quantum network architecture as a viable solution for metropolitan scales. With a fully deployable QKD system, which is particularly suitable for ad hoc implementation in scenarios where fibre connections are infeasible, we demonstrated all the main building blocks of such a network. We achieved up to 5.7 kbps secure key rates over two different links and under various link conditions, with over 2.5 kbps in full daylight, indicating that the system has a potential for 24/7 operation. To our knowledge, this is the first demonstration of kbps-rate free-space QKD over kilometre distances with an entanglement-based approach. Moreover, it is an improvement of entanglement-based QKD daylight capability by an order of magnitude in both secret key rate and link range[27]. The results are also competitive with prepare-and-measure systems. With our large-aperture free-space terminals, specifically designed for metropolitan applications, we estimate kbps key rates are possible even over 10-km links. A full coverage of a city is therefore within reach with the present technology.

By implementing the quantum channel at 810 nm, we break with ongoing trends of transferring the free-space segments to telecom C band wavelengths. Network architectures implemented in C band typically strive to minimize the number of detectors[4,43], which is due to the fact that single-photon detection at 1550 nm is a cost driver. This does not apply in our case, where transmitter and receiver systems are of similar cost and complexity. However, 1550 nm will almost certainly remain the wavelength of choice for long fibre segments due to a substantially lower loss. A non-degenerate entangled photon source[44], which emits photons at 1550 nm and 810 nm, could therefore act as an elegant interface between fibre and free-space segments of a heterogeneous network.

There are many possible improvements to the present system on the horizon. Extending the two-user scenario to a fully connected multi-user network is straightforward with the latest multiplexing techniques[13,16,20]. By combining such a multiplexing scheme together with our system, we estimate kbps nighttime and hundreds of bps daytime rates are possible for a multi-user scenario with multiple 1.7 km free-space links. Sources that are capable of providing a large spectral bandwidth for multiplexing have been recently demonstrated, for example by Lohrmann et al.[45] Recent developments towards ultra-bright GHz rate entangled pair sources[45–47] show that a single entanglement server could support many end users.

Adaptive optics (AO) could significantly improve daylight performance by reducing the effective focal spot size and thus giving the possibility for tighter spatial filtering[35,38]. Furthermore, with efficient AO-enabled single-mode fibre coupling, hybrid free-space-to-fibre quantum links become possible. This would allow for physical separation of the end user from the receiver free-space terminal, introducing considerably more flexibility. Entanglement swapping[39] would not only increase the extent of the present network without the need for trusted nodes, but it would also enable integration into larger heterogeneous networks that employ fundamentally different forms of entanglement[21].

Another way forward is to exploit high-dimensional entanglement, which promises higher information capacity per photon, better security, and enhanced robustness to noise[48,49]. Although the practicality of orbital angular momentum (OAM) modes remains questionable for long-distance free-space communication[50], the OAM-entanglement might still be well suited for metropolitan distances[51]. AO would further improve key rates by protecting spatial mode entanglement from the influence of atmospheric turbulence[52]. An entangled photon source can also generate hyperentanglement—simultaneous entanglement in different degrees of freedom—quite naturally[53], which could be

used to make a single server compatible with a range of receiver types. A recent experiment demonstrates that extending entanglement into the time-bin degree of freedom could also significantly boost secure key rates[54].

Finally, the distribution of entanglement lies at the heart of many applications beyond QKD. Practical and efficient metropolitan entanglement distribution networks would therefore facilitate the development of entirely new applications at the intersection of distributed sensing and quantum information processing, such as quantum clock synchronization[55], long baseline interferometry[56], and multi-partite quantum cryptography[57,58].

METHODS

Entanglement server

Our entanglement server (ES) consists of an entangled photon source, which generates bipartite polarization entanglement. It is based on spontaneous parametric down conversion (SPDC) in a periodically poled potassium titanyl phosphate (ppKTP) crystal, employing an intrinsically phase-stable Sagnac configuration[59]. The poling period of the nonlinear crystal was chosen to ensure a type-II quasi-phase matching at a temperature of approximately 30 °C for a pump wavelength of 405 nm and near-degenerate downconversion wavelengths around 810 nm. The temperature and pump wavelength were stabilized using standard temperature and current controllers. The generated entangled pair state is of the form

$$|\Psi\rangle \propto |H_s\rangle|V_i\rangle + \beta e^{i\varphi}|V_s\rangle|H_i\rangle, \tag{1}$$

where H and V are horizontal and vertical polarization states, and subscripts s and i stand for signal and idler paths. Coefficients β and φ are adjusted by manipulating the polarization of the pump to achieve a maximally entangled Bell state that we use for QKD.

During our experiments, the intrinsic photon pair generation rate (before any loss is considered) in the ES was estimated to be approximately 12 million pairs per second, over a spectral bandwidth of 0.45 nm (FWHM). These results match well the expected performance for the 30-mm-long ppKTP crystal used in the experiment. Visibilities of up to 99.5% and 97.4% were measured in the low pump power limit for horizontal-vertical and diagonal-antidiagonal basis, respectively. The source was built on an optical breadboard and housed in a wheeled 19-inch rack. We note that there was no temperature stabilization for the environment of the breadboard.

Quantum receiver subsystem

We developed two complete quantum receiver subsystems (QRS), one for Alice and one for Bob, for performing QKD based on the BBM92 protocol[41]. Each QRS consists of a standard polarization analysis module (PAM), 4 single-photon avalanche diodes (SPADs), time-tagging electronics, a rubidium clock, and units for post-processing. In the PAMs, we realized the randomized basis selection with a 50:50 beam splitter. We note, that this splitting ratio is not optimal and that by using a biased basis randomization, the final secure key rate could be further improved, albeit only slightly[29]. We used commercial single-photon avalanche diodes (SPADs) with detection efficiency of >60%, dark count rate of <500 cps, and timing resolution of 350 ps. To ensure matching of polarization frames of reference at Alice and Bob, a QRS also incorporates a waveplate-based polarization controller. For the night experiment, polarization basis alignment was performed right before the experiment, while for the daytime experiment, it was performed the night before, since the absence of background noise allowed for better initial alignment. See Supplementary Note 2 for more information about the QRS.

Alice's QRS is almost identical to the QRS of Bob—the only difference is in its PAM, which is a much more compact and simplified version of Bob's. This is because Alice detects photons that are coming from the server via a single-mode fibre and is therefore not exposed to the free-space link environment and related challenges. Bob's PAM, on the other hand, incorporates additional spatial and spectral filters for daylight operation, as discussed in the next section. The complete QRS of Alice was housed in a wheeled 19-inch rack, while Bob's PAM was mounted directly onto the receiver free-space terminal and the rest of his QRS was housed in a rack.

Daylight noise filtering

Noise suppression turns out to be of critical importance in a free-space channel, particularly during daytime, when atmospheric scattering of sunlight can cause the receiver telescope to collect noise photons at rates that are many orders of magnitude higher than the signal photon rates. To reduce the noise, we employ filtering in all three degrees of freedom: spectral, spatial, and temporal. Spectral filtering is realized with a stack of commercial interference filters, resulting in a 3 nm wide pass-band (FWHM) around the signal wavelength of 810 nm.

The spatial filter consists of a Keplerian telescope with a small adjustable opening in its focal plane, which has the effect of reducing the overal receiver system field of view (FOV)[60,61]. The adjustable spatial filtering module is discussed in detail in ref. [62]. For our daylight experiments, we thus reduced the system FOV to 31 μrad, which was just large enough to transmit the majority of the signal, while blocking considerable amounts of noise. For comparison, this FOV is 2 orders of magnitude smaller than the FOV of our receiver telescope, resulting in a noise reduction by 4 orders of magnitude (noise rate scales with the square of the linear FOV), assuming a uniform distribution of noise over the FOV. For the nighttime experiment, when the background noise was negligible, the adjustable spatial filter was fully opened and the limiting field stop became the core of the multi-mode fibres in PAM, which resulted in the system FOV of about 52 μrad. Using single-mode instead of multi-mode coupling would, indeed, offer unparalleled rejection of noise in daylight. However, having no high-order adaptive optics, signal wavefront distortions due to atmospheric turbulence would substantially deteriorate coupling efficiency of the signal in the single-mode case[63]. Such signal loss would for many link conditions be too high of a price to pay for the achieved reduction of noise, which is particularly obvious for using the system at nighttime, when the background noise is at a negligible level. Our approach, on the other hand, allows using the more relaxed multi-mode coupling in low-noise conditions, while imposing a narrower FOV as the noise increases[62].

Spectral and spatial filter modules were directly integrated into Bob's quantum receiver subsystem. Temporal filtering, on the other hand, comes with the coincidence-based detection. For both experiments here, coincidence window of 1 ns was used. Note, that this was near-optimal for the night experiment, however, its optimization in daytime could improve the achievable secure key rates. Furthermore, comparing our signal and filter spectra shows that we could employ at least a 3-times narrower spectral filter, reducing the noise by a factor of 3 while not considerably affecting the signal throughput.

Free-space terminals

We developed two portable and highly versatile optical free-space terminals[64]. For the experiments presented here, we used the 810 nm channel for the quantum signal and the 1064 nm channel for the beacon laser, and the beam stabilization subsystem at the receiver terminal. Both terminals incorporate identical transceiver telescopes, which are based on an afocal three-mirror anastigmat (TMA) design combined with an additional fourth mirror to reduce
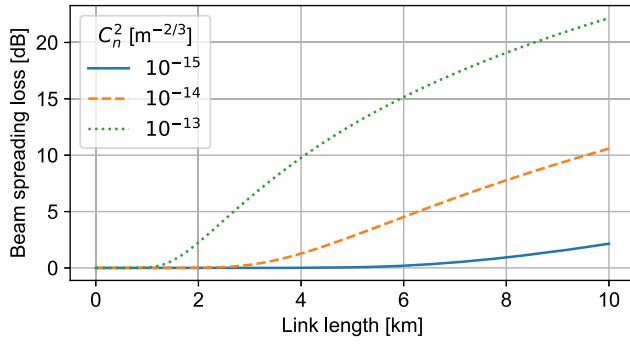
Fig. 4 Estimated link loss due to diffraction and turbulence induced beam spreading. The loss is shown for three different turbulence strengths, characterized by refractive index structure parameter C_n^2.

the size and improve the optical quality. The efficiency of each transceiver telescope is about 73% at 810 nm. The off-axis telescope layout renders the transceiver system with high signal throughput due to the absence of a central obscuration. The shape of the individual mirrors is designed to provide diffraction-limited performance over the full telescope aperture of 200 mm and the entire FOV of 3.5 mrad. After mirror manufacturing and system integration, the wavefront RMS error for the two telescopes was slightly worse, namely about 100 nm and 150 nm, measured at 632.8 nm. Note that this value corresponds to the full aperture, meaning that when a smaller portion of it is used, such as was the case on the transmitter side in our experiments, the wavefront error would be considerably smaller. For example, over a subaperture of 40 mm, the measured wavefront RMS error was less than 20 nm for both telescopes.

Furthermore, such a large aperture prevents severe signal loss due to diffraction and atmospheric turbulence even over link distances of several kilometres. For the transmitter beam waist of 40 mm and the receiver aperture diameter of 200 mm, both corresponding to our system, we calculated the long-term average loss associated with clipping of the beam at the receiver telescope aperture, using a well-established approach to model beam spreading after propagating through Kolmogorov turbulence[65]. This loss due to beam spreading, which considers both turbulence-induced spreading as well as diffraction, is shown in Fig. 4 for a range of link lengths and different turbulence strengths. We can see that for a 1.7 km link under medium turbulence with refractive index structure parameter $C_n^2 = 10^{-15}$ m$^{-2/3}$, the beam spreading loss is essentially zero. Even for a 10 km link and the same C_n^2, the beam spreading loss would still be as low as 2.1 dB, clearly making these terminals particularly suitable for low-loss free-space links over metropolitan distances. For more technical details about the terminals, we refer the reader to ref. [64].

Post-processing and secure key rate calculation
The first step of post-processing is to read data from the time-taggers. Alice and Bob exchange lists of time tags and conduct time synchronization in two steps. First, a progressive cross-correlation-based pre-synchronization algorithm with complexity $O(n \log n)$ is used to establish an initial clock offset over a wide range of multiple seconds. Once a coarse offset is found, fine synchronization works on a smaller block size that depends on the number of detections (see Supplementary Note 3). For a more detailed discussion of similar approaches, we refer the reader to ref. [66].

The sifting stage compares the measurement bases of the detections and keeps only events that share the same basis. The error estimation stage discloses a fraction of 10% of sifted key data in order to estimate the error rate in the quantum channel. Note, that the fraction of disclosed bits can be optimized to increase the amount

of secure key, however, this was beyond the scope of experiments here. Information reconciliation (error correction) is then performed according to the cascade protocol[67] so that Alice and Bob agree on the same key with a probability close to one. The subsequent confirmation stage tests whether information reconciliation was successful, i.e. it ensures the correctness of Alice's and Bob's key up to a minor error probability ε_{corr} (the probability that Alice's and Bob's key differ and the confirmation stage does *not* detect it). For each key, Alice and Bob choose at random a hash function from a family of universal polynomial hash functions and calculate, exchange, and compare a hash of $t = 96$ bits of their reconciled key data. This results in $\varepsilon_{corr} = \frac{m-k}{t} 2^{-t}$, where m is the number of bits after sifting and k is the number of bits disclosed during error estimation.

For the experimental results reported here, all of the above was done online during the experiments. Secure key rates, taking into account also finite key effects, were then calculated offline using the security proof from ref. [68]. The length of the secure keys is given as

$$l = \mathrm{floor}\left[(m-k)(1 - h_2(\delta + v)) - r - t - 2a + 2\log_2(2\varepsilon_{pa})\right],$$
(2)

with

$$v = \sqrt{\frac{m(k+1)}{(m-k)k^2} \ln\left(\frac{2}{\varepsilon_{pe}}\right)},$$
(3)

where r is the number of bits disclosed during information reconciliation, δ is the error rate threshold for the parameter estimation test, ε_{pa} is the accepted failure probability due to privacy amplification, and ε_{pe} is the accepted probability that the actual error rate is larger than $\delta + v$, given that the parameter estimation test has been passed. We also introduced a, which corresponds to the length of the one-time pads used for encryption of authentication tags (the factor 2 represents one tag for each direction), since the original security proof assumes an authentic channel. We performed calculations on data blocks corresponding to 5-min measurement times, with $\delta = 0.034$ and $a = 96$, and chose the total failure probability of the QKD protocol over an authentic channel $\varepsilon_{qkd} = 10^{-11}$. We further set $\varepsilon_{pa} = \varepsilon_{qkd} \times 10^{-3}$ and $\varepsilon_{pe} = \varepsilon_{qkd} - \varepsilon_{pa} - \varepsilon_{corr}$. The overall security of the calculated keys can be finally assessed by the parameter ε, which takes the authentication into account, and the fact that a part of the QKD keys is used for the authentication of the next round. ε grows with the number of processed data blocks n as[69,70]

$$\varepsilon \leq n(\varepsilon_{qkd} + \varepsilon_{auth}),$$
(4)

with $\varepsilon_{auth} = \frac{C}{a} 2^{-a}$, where C is the length of the authenticated classical communication exchanged (in bits).

While these results were calculated offline, we note that the system is fully capable of live on-the-fly secure key generation. The system can implement the necessary steps, including delayed authentication according to ref. [71] with polynomial universal hashing over GF(2^{96}) with a pre-shared secret key, and privacy amplification using a Toeplitz matrix approach. The estimated rates reported here closely match the rate of secure keys generated live.

System efficiencies
To calculate system efficiencies, we adapt the model from ref. [72]. We first determine the coincidence-window-dependent detection efficiency

$$\eta_{coin} = \mathrm{erf}\left[\sqrt{\ln(2)} \frac{\tau}{t_\Delta}\right],$$
(5)

where τ is the coincidence window and t_Δ is the full width at half maximum of the $g^{(2)}$ function, i.e. the correlation between Alice and Bob's detector clicks. Since t_Δ primarily depends on the time

jitter of the detectors, we regard it as a constant of our system. We measured its value to be $t_\Delta = 710 \pm 8$ ps. Together with $\tau = 1$ ns, this results in η_{coin} of about 83.8%. During the experiments, we were using 10% of the detection events for estimating Alice and Bob's single detection rate S_{det}^a and S_{det}^b, respectively, and the coincidence detection rate C_{det} (these events are excluded from the key calculation). We calculate the true coincidence rate as

$$C_{true} = \frac{C_{det} - C_{acc}}{\eta_{coin}}, \tag{6}$$

where the accidental coincidence rate is estimated as

$$C_{acc} = S_{det}^a S_{det}^b \tau. \tag{7}$$

Furthermore, by subtracting the dark count rate S_{DC}^i and the background noise rate S_{BG}^i from the detected single rates, we arrive at the contribution of the true (signal) photons,

$$S_{sig}^i = S_{det}^i - S_{DC}^i - S_{BG}^i, \tag{8}$$

where superscript $i \in \{a, b\}$ stands for Alice or Bob. We may then determine the total system efficiencies for Alice and Bob (sometimes called heralding efficiencies) as

$$\eta^a = \frac{C_{true}}{S_{sig}^b}, \eta^b = \frac{C_{true}}{S_{sig}^a}. \tag{9}$$

These system efficiencies account for all the single channel losses from the moment a pair is created until it gets processed by the software, therefore it includes also intrinsic ES and detector efficiencies. The dark count rates are also regarded as system constants and we measured them to be $S_{DC}^a = (1,702 \pm 21)$ cps and $S_{DC}^b = (761 \pm 7)$ cps, on average.

For the night experiment, background count rate was negligible, therefore we can set S_{BG}^a and S_{BG}^b to zero. This allows us to use the model above to characterize η^a and η^b. They are found to be very stable throughout the experiment, with the mean and standard deviation of $(8.90 \pm 0.03)\%$ for Alice, and $(1.63 \pm 0.08)\%$ for Bob. For the daytime experiment, we can estimate η^b in the same way, since Alice's channel was fully fibre-based and thus experienced negligible background count rates. Doing so results in $\eta^b = (1.25 \pm 0.35)\%$. On the other hand, Bob's background was far from negligible during this experiment, therefore we cannot extract η^a in the same way. However, while η^b depends on the link conditions that may considerably change throughout the day, η^a is not expected to considerably change for days. We therefore characterized it the night before, arriving at $\eta^a = (8.13 \pm 0.09)\%$. The lower mean and the higher standard deviation of η^b for the daytime experiment is not surprising, since narrowing down the spatial filter incurred additional loss and increased link efficiency fluctuations due to atmospheric turbulence. Note, that the source was realigned just before the night experiment, hence a slightly better η^a then.

While the individual contributions to the total system efficiencies were not monitored during the experiments, we characterized the total efficiency of the classical free-space link on another occasion in comparable link conditions, which was around 30–35% for 810 nm. This includes efficiency of both telescopes, both tip-tilt correction systems, all the additional optics in the free-space terminals and in the quantum receiver subsystem, as well as multi-mode coupling efficiency at the receiver, with the latter of about 80%. The total system efficiencies reported above further include the quantum source and single-photon detector efficiencies.

Solar radiation and background count rate

To quantify sky brightness during our experiments, solar radiation data was extracted from the publically available database of the University of Applied Sciences Jena (http://wetter.mb.eah-jena.de/ station/index.html). The measurements were performed using a pyranometer, which measures total incident solar radiation over the whole hemisphere in the spectral band between 300 nm and 2.8 μm. The pyranometer was located approximately 1.2 km from Alice and approximately 2.6 km from Bob. Although not measured exactly where our experiments took place, and despite being measured over a much broader spectral range compared to our QKD spectral filter bandwidth, it still offers a reasonable metric for quantifying system-independent sky brightness at the link. This is evident from its corellation with the detected daylight noise (Fig. 3), which we estimate in the following way. As above, we determine the true coincidence rate C_{true} from the detected rates. This time, however, S_{det}^b also consists of a considerable contribution of S_{BG}^b due to daylight. Using η^a that was determined the night before, we can estimate S_{sig}^b from C_{true} and with it extract S_{BG}^b from S_{det}^b, following the relations given above.

Performance estimation for a 10 km link

Extending the free-space link to longer distances would introduce an additional loss factor of η to Bob's signal channel. Using the secure key rate model from ref. [72], it is straightforward to show that in the limit of much larger received signal rates compared to noise rates, key rates would scale linearly with η. During our night experiment, we achieved a mean secure key rate of 5.4 kbps, while the estimated mean total count rate at Alice and Bob was 1.0 Mcps and 190 kcps, respectively. During this experiment, total noise count was less than 2 kcps for Alice and less than 1 kcps for Bob, consisting mostly of dark count. For a 10-km link, where we estimate $\eta = 10^{-2.1/10} \approx 0.62$ as discussed above (see Fig. 4), we can therefore assume linear scaling of the key rate with η and thus expect 3.3 kbps key rate to be achievable with our system in nighttime. Note that the loss due to atmospheric scattering and absorption is assumed to be negligible.

Extrapolation to multiple free-space link scenarios

To estimate achievable key rates in a dual free-space link scenario (two 1.7 km free-space links with ES in the middle), we take Bob's channel parameters and count rates extracted from our experiments and assume the same for Alice's channel. In particular, we first extract η^b and S_{sig}^b for our system, as explained above. Together with the directly measured S_{det}^b, we may then estimate true and accidental coincidence rate in such a scenario as

$$C_{true}^{(a \sim b)} = \eta^b S_{sig}^b \tag{10}$$

and

$$C_{acc}^{(a \sim b)} = \left(S_{det}^b\right)^2 \tau. \tag{11}$$

Imperfections in the ES, PAMs, and alignment of the polarization frames of reference at Alice and Bob lead to occasional erroneous polarization measurements[72]. We extract the rate at which this happens from the experimental data as

$$e_{pol} = \frac{C_{err} - C_{acc}/4}{C_{sift}}, \tag{12}$$

where C_{err} is the sum of measured coincidences in the wrong channels and C_{sift} are the total measured coincidences after sifting. Finally, we assume a constant error correction efficiency of 1.1 (which is very close to the values achieved during our experiments) and estimate the key in the asymptotic limit according to the model in ref. [72].

We can also extend these results to a multiple free-space link scenario based on wavelength division multiplexing, which was already demonstrated to work well in optical fibres[13,16]. Here, each of the u users in the network establishes a secure key pairwise with every other user, resulting in $k = u(u - 1)/2$ different secret keys generated in parallel. Since each pair of channels connecting

any two users is independent from every other user pair, this means that a fraction G/k of the intrinsic ES pair generation rate G is used for generation of each key, assuming the ES emission spectrum can be uniformly distributed over the multiplexed wavelength channels for simplicity. Employing such wavelength division multiplexing and a k-fold increase of the ES pump power, we would therefore arrive at the same key rate predictions for a multiple free-space link case as in the dual free-space link case, assuming all the free-space links are identical.

DATA AVAILABILITY

The data presented in the figures and that support the findings of this study are available from the corresponding authors on reasonable request.

CODE AVAILABILITY

The code used for data processing is available from the corresponding authors on reasonable request.

REFERENCES

1. Krenn, M., Malik, M., Scheidl, T., Ursin, R. & Zeilinger, A. In *Optics in Our Time* (eds Al-Amri, M. D., El-Gomati, M. & Zubairy, M. S.) 455–482 (Springer International Publishing, 2016).
2. Wehner, S., Elkouss, D. & Hanson, R. Quantum internet: A vision for the road ahead. *Science* **362** (2018).
3. Zhang, Q., Xu, F., Chen, Y.-A., Peng, C.-Z. & Pan, J.-W. Large scale quantum key distribution: challenges and solutions Invited. *Opt. Express* **26**, 24260–24273 (2018).
4. Chen, Y.-A. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **589**, 214–219 (2021).
5. Liao, S.-K. et al. Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017).
6. Yin, J. et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.* **119**, 200501 (2017).
7. Liao, S.-K. et al. Satellite-relayed intercontinental quantum network. *Phys. Rev. Lett.* **120**, 30501 (2018).
8. Yin, J. et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* **582**, 501–505 (2020).
9. Lu, C.-Y., Cao, Y., Peng, C.-Z. & Pan, J.-W. Micius experiments in space. *Rev. Mod. Phys.* **94**, 33 (2022).
10. Li, Z.-D. et al. Experimental quantum repeater without quantum memory. *Nat. Photonics* **13**, 644–648 (2019).
11. Pu, Y.-F. et al. Experimental demonstration of memory-enhanced scaling for entanglement connection of quantum repeater segments. *Nat. Photonics* **15**, 374–378 (2021).
12. Langenfeld, S., Thomas, P., Morin, O. & Rempe, G. Quantum repeater node demonstrating unconditionally secure key distribution. *Phys. Rev. Lett.* **126**, 230506 (2021).
13. Joshi, S. K. et al. A trusted node-free eight-user metropolitan quantum communication network. *Sci. Adv.* **6** (2020).
14. Dynes, J. F. et al. Cambridge quantum network. *npj Quantum Inf.* **5**, 2728 (2019).
15. Chen, T.-Y. et al. Implementation of a 46-node quantum metropolitan area network. *npj Quantum Inf.* **7**, 661 (2021).
16. Wengerowsky, S., Joshi, S. K., Steinlechner, F., Hübel, H. & Ursin, R. An entanglement-based wavelength-multiplexed quantum communication network. *Nature* **564**, 225–228 (2018).
17. Bunandar, D. et al. Metropolitan quantum key distribution with silicon photonics. *Phys. Rev. X* **8** (2018).
18. Valivarthi, R., Etcheverry, S., Aldama, J., Zwiehoff, F. & Pruneri, V. Plug-and-play continuous-variable quantum key distribution for metropolitan networks. *Opt. Express* **28**, 14547–14559 (2020).
19. Alshowkan, M. et al. Reconfigurable quantum local area network over deployed fiber. *PRX Quantum* **2**, 503 (2021).
20. Appas, F. et al. Flexible entanglement-distribution network with an AlGaAs chip for secure communications. *npj Quantum Inf.* **7**, 715 (2021).
21. Guccione, G. et al. Connecting heterogeneous quantum networks by hybrid entanglement swapping. *Sci. Adv.* **6** (2020).

22. Sidhu, J. S. et al. Advances in space quantum communications. *IET Quantum Commun.* **2** (2021).
23. Peng, C.-Z. et al. Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication. *Phys. Rev. Lett.* **94**, 150501 (2005).
24. Marcikic, I., Lamas-Linares, A. & Kurtsiefer, C. Free-space quantum key distribution with entangled photons. *Appl. Phys. Lett.* **89**, 101122 (2006).
25. Ursin, R. et al. Entanglement-based quantum communication over 144 km. *Nat. Phys.* **3**, 481–486 (2007).
26. Erven, C., Couteau, C., Laflamme, R. & Weihs, G. Entangled quantum key distribution over two free-space optical links. *Opt. Express* **16**, 16840–16853 (2008).
27. Peloso, M. P., Gerhardt, I., Ho, C., Lamas-Linares, A. & Kurtsiefer, C. Daylight operation of a free space, entanglement-based quantum key distribution system. *N. J. Phys.* **11**, 45007 (2009).
28. Erven, C. et al. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *N. J. Phys.* **14**, 123018 (2012).
29. Cao, Y. et al. Entanglement-based quantum key distribution with biased basis choice via free space. *Opt. Express* **21**, 27260–27268 (2013).
30. Ecker, S. et al. Strategies for achieving high key rates in satellite-based QKD. *npj Quantum Inf.* **7**, 163 (2021).
31. Basso Basset, F. et al. Quantum key distribution with entangled photons generated on demand by a quantum dot. *Sci. Adv.* **7** (2021).
32. Mishra, S. et al. BBM92 quantum key distribution over a free space dusty channel of 200 meters. *J. Opt.* **24**, 74002 (2022).
33. Basso Basset, F. et al. Daylight entanglement-based quantum key distribution with a quantum dot source. *Quantum Sci. Technol.* **8**, 025002 (2023).
34. Liao, S.-K. et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nat. Photonics* **11**, 509–513 (2017).
35. Gong, Y.-H. et al. Free-space quantum key distribution in urban daylight with the SPGD algorithm control of a deformable mirror. *Opt. Express* **26**, 18897–18905 (2018).
36. Cao, Y. et al. Long-distance free-space measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **125**, 260503 (2020).
37. Avesani, M. et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *npj Quantum Inf.* **7**, 145 (2021).
38. Gruneisen, M. T. et al. Adaptive-optics-enabled quantum communication: a technique for daytime space-to-earth links. *Phys. Rev. Appl.* **16**, 126111 (2021).
39. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012 (2020).
40. Herbst, T. et al. Teleportation of entanglement over 143 km. *Proc. Natl Acad. Sci. USA* **112**, 14202–14205 (2015).
41. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68**, 557–559 (1992).
42. Andrews, L. C. & Phillips, R. L. *Laser Beam Propagation through Random Media* (SPIE, 2005).
43. Fröhlich, B. et al. A quantum access network. *Nature* **501**, 69–72 (2013).
44. Hentschel, M., Hübel, H., Poppe, A. & Zeilinger, A. Three-color Sagnac source of polarization-entangled photon pairs. *Opt. Express* **17**, 23153–23159 (2009).
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**, 21101 (2020).
46. Cao, Y. et al. Bell test over extremely high-loss channels: towards distributing entangled photon pairs between earth and the Moon. *Phys. Rev. Lett.* **120**, 140405 (2018).
47. Steiner, T. J. et al. Ultrabright entangled-photon-pair generation from an AlGaAs-on-insulator microring resonator. *PRX Quantum* **2**, 1 (2021).
48. Forbes, A. & Nape, I. Quantum mechanics with patterns of light: Progress in high dimensional and multidimensional entanglement with structured light. *AVS Quantum Sci.* **1**, 11701 (2019).
49. Erhard, M., Krenn, M. & Zeilinger, A. Advances in high-dimensional quantum entanglement. *Nat. Rev. Phys.* **2**, 365–381 (2020).
50. Krenn, M. et al. Twisted light transmission over 143 km. *Proc. Natl Acad. Sci. USA* **113**, 13648–13653 (2016).
51. Krenn, M., Handsteiner, J., Fink, M., Fickler, R. & Zeilinger, A. Twisted photon entanglement through turbulent air across Vienna. *Proc. Natl Acad. Sci. USA* **112**, 14197–14201 (2015).
52. Sorelli, G., Leonhard, N., Shatokhin, V. N., Reinlein, C. & Buchleitner, A. Entanglement protection of high-dimensional states by adaptive optics. *N. J. Phys.* **21**, 23003 (2019).
53. Barreiro, J. T., Langford, N. K., Peters, N. A. & Kwiat, P. G. Generation of hyperentangled photon pairs. *Phys. Rev. Lett.* **95**, 260501 (2005).
54. Chapman, J. C., Lim, C. C. W. & Kwiat, P. G. Hyperentangled time-bin and polarization quantum key distribution. *Phys. Rev. Appl.* **18**, 044027 (2022).
55. Ilo-Okeke, E. O., Tessler, L., Dowling, J. P. & Byrnes, T. Remote quantum clock synchronization without synchronized clocks. *npj Quantum Inf.* **4**, 281 (2018).

56. Gottesman, D., Jennewein, T. & Croke, S. Longer-baseline telescopes using quantum repeaters. *Phys. Rev. Lett.* **109**, 70503 (2012).

57. Proietti, M. et al. Experimental quantum conference key agreement. *Sci. Adv.* **7** (2021).

58. Thalacker, C., Hahn, F., Jong, J., de, Pappa, A. & Barz, S. Anonymous and secret communication in quantum networks. *N. J. Phys.* **23**, 83026 (2021).

59. Kim, T., Fiorentino, M. & Wong, F. N. C. Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. *Phys. Rev. A* **73** (2006).

60. Gruneisen, M. T. et al. Adaptive spatial filtering of daytime sky noise in a satellite quantum key distribution downlink receiver. *Opt. Eng.* **55**, 26104 (2016).

61. Ko, H. et al. Experimental filtering effect on the daylight operation of a free-space quantum key distribution. *Sci. Rep.* **8**, 15315 (2018).

62. Kržič, A., Döll, N., Chandrashekara, U., Spiess, C. & Steinlechner, F. Adjustable spatial filter for optimal free-space quantum communication round the clock. Preprint at https://arxiv.org/abs/2303.09942. (2023).

63. Dikmelik, Y. & Davidson, F. M. Fiber-coupling efficiency for free-space optical communication through atmospheric turbulence. *Appl. Opt.* **44**, 4946–4952 (2005).

64. Goy, M. et al. High performance optical free-space links for quantum communications. In *Proceedings, International Conference on Space Optics — ICSO 2020*, Vol. 11852 (eds Cugny, B., Sodnik, Z. & Karafolas, N.) (SPIE, 2021).

65. Andrews, L. C. *Field Guide to Atmospheric Optics* (SPIE Press, 2019).

66. Spiess, C. et al. Clock synchronization with correlated photons. *Phys. Rev. Appl.* **19**, 054082 (2023).

67. Martinez-Mateo, J., Pacher, C., Peev, M., Ciurana, A. & Martin, V. Demystifying the information reconciliation protocol cascade. *Quantum Inf. Comput* **15**, 0453–0477 (2015).

68. Tomamichel, M. & Leverrier, A. A largely self-contained and complete security proof for quantum key distribution. *Quantum* **1**, 14 (2017).

69. Müller-Quade, J. & Renner, R. Composability in quantum cryptography. *N. J. Phys.* **11**, 085006 (2009).

70. Portmann, C. & Renner, R. Security in quantum cryptography. *Rev. Mod. Phys.* **94**, 025008 (2022).

71. Pacher, C., Lechner, G., Portmann, C., Maurhart, O. & Peev, M. Efficient QKD postprocessing algorithms. Poster presented at: *2nd Annual Conference on Quantum Cryptography (QCrypt)* (Singapore, 2012).

72. Neumann, S. P. et al. Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources. *Phys. Rev. A* **104**, 226 (2021).

AUTHOR CONTRIBUTIONS

FUNDING

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/s41534-023-00754-0.

Correspondence and requests for materials should be addressed to Andrej Kržič or Fabian Steinlechner.

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.